Consortium GARR

Workshop GARR_14
Selected papers

NEXT NETWORK
COSTRUIAMO IL FUTURO DELLA RETE

Roma, 2-4 dicembre 2014

Consortium GARR

Workshop GARR 2014
Selected papers

NEXT NETWORK

COSTRUIAMO IL FUTURO DELLA RETE

Roma, 2-4 dicembre 2014

ISBN 978-88-905077-5-5

Editore: Associazione Consortium GARR
Via dei Tizii, 6, 00185 Roma, Italia
http://www.garr.it
Tutti i diritti riservati.

Curatori editoriali: Marta Mieli, Maddalena Vario, Carlo Volpe
Progetto grafico: Carlo Volpe
Impaginazione: Marta Mieli, Carlo Volpe

Prima stampa: Marzo 2016
Numero di copie: 600
Stampa: Tipografia Graffietti Stampati snc
S.S. Umbro Casentinese Km 4.500, 00127 Montefiascone (Viterbo)

Tutti i materiali relativi al Workshop GARR 2014 sono disponibili all'indirizzo: http://www.garr.it/ws14

Indice

Introduzione

Claudia Battista

Chair del Comitato di Programma del Workshop GARR 2014

L'edizione 2014 del Workshop GARR ha rappresentato un gradito ritorno. Dopo alcuni anni di assenza, l'appuntamento dedicato ai professionisti del settore ICT e referenti tecnici della rete GARR è stato un'occasione di incontro e di approfondimento su temi sui quali ci si confronta ogni giorno.

Il titolo "Next Network. Costruiamo il futuro della rete" descrive bene il focus principale dell'evento. L'attenzione è stata posta sulle attività che nelle nostre università e centri di ricerca si conducono quotidianamente e sulle sfide cui gli utenti sono chiamati a confrontarsi per gestire le reti informatiche, i servizi e le applicazioni che sono sempre più determinanti per il successo della ricerca e della didattica. Si tratta di una rete che cresce con il contributo di tutti: non una infrastruttura fornita dall'alto, ma costruita appunto in maniera collaborativa e condivisa.

Lo sguardo, come sempre, è rivolto al futuro. Next Network, appunto. Perché la rete della ricerca non si ferma mai e cerca di anticipare le esigenze degli utilizzatori, delineando nuovi orizzonti e tracciando strade tecnologicamente all'avanguardia.

Durante le tre giornate dell'evento ci sono state discussioni importanti che hanno fatto riflettere sul ruolo che la comunità accademica e della ricerca dovrebbe avere nella conservazione e nello sviluppo di competenze, che sempre più rischiano di scomparire di fronte a colossi commerciali, nel nome della revisione della spesa. Sono state dibattute questioni che restano ancora aperte come l'opportunità di affidare in outsourcing la gestione di servizi fondamentali, quali ad esempio il servizio di posta elettronica.

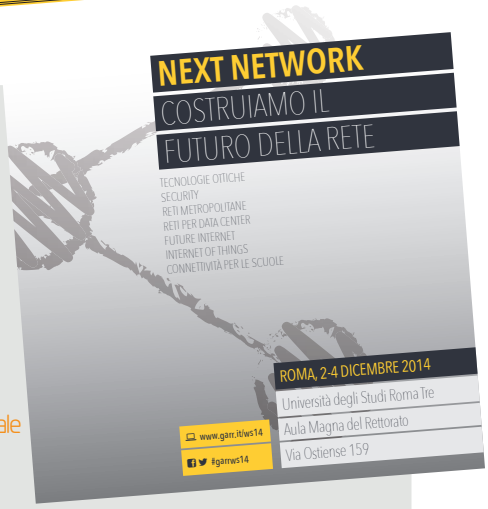
Altro tema molto attuale è quello relativo alla proprietà dei dati e alla tutela delle informazioni personali nel cloud computing. Durante l'evento è stata offerta una panoramica circa le definizioni, i modelli e i servizi offerti in modalità cloud, soffermandosi sulle criticità relative alla proprietà delle infrastrutture e del software ed al rapporto tra utente e fornitore.

Sono stati affrontati i temi della sicurezza informatica: dagli attacchi DDoS, all'accesso alle reti WiFi non cifrate, all'autorizzazione federata. Si è parlato di Future Internet, Internet of Things, IPv6, Building automation e reti per datacenter.

Una sessione del programma, inoltre, è stata dedicata ai modelli di connettività per le scuole. Si tratta di un argomento che riguarda sempre più da vicino la comunità GARR che si è ampliata notevolmente negli ultimi anni grazie al collegamento di centinaia di istituti scolastici in tutta Italia.

Ringraziando tutti i partecipanti e coloro che hanno permesso il buon successo del Workshop, a partire dal comitato di programma, che ha selezionato i seguenti contributi, vi auguro una buona lettura.

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR



Chair del Workshop

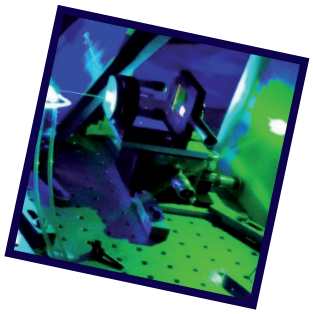
Claudia Battista, GARR

Comitato di programma

Claudio Allocchio, GARR
Mauro Campanella, GARR
Massimo Carboni, GARR
Paolo Caturegli, Università degli Studi di Pisa
Roberto Cecchini, GARR e INFN
Marco D'Ambrosio, Università degli Studi di Cassino e del Lazio Meridionale
Paolo De Rosa, Università degli Studi di Pisa
Giancarlo Galluzzi, Università degli Studi di Milano
Marco Sommani, CNR
Massimo Tartarella, Università degli Studi di Palermo
Gloria Vuagnin, GARR
Stefano Zani, INFN

Tutte le presentazioni e maggiori informazioni sono disponibili sul sito dell'evento:
www.garr.it/ws14

L'orologio atomico distribuito su fibra ottica



Davide Calonico

INRIM, Istituto Nazionale di Ricerca Metrologica

Abstract. La fibra ottica per disseminare sul territorio gli orologi campioni dell'Istituto Nazionale di Ricerca Metrologica, portando in laboratori remoti un'accuratezza senza precedenti.
Cosa succederebbe se la precisione degli orologi primari nazionali dell'Istituto Nazionale di Ricerca Metrologica (INRIM), potesse essere trasferita in fibra a un laboratorio distante centinaia di chilometri in pochi istanti? Quali benefici se ne trarrebbero nell'immediato, e cosa accadrà in futuro?

A Torino si trova l'orologio campione nazionale che realizza la definizione del secondo nel Sistema Internazionale delle misure, dapprima presso l'Istituto Elettrotecnico Nazionale "Galileo Ferraris", e dal 2006 all'INRIM, nato dall'unione del "G. Ferraris" con l'Istituto di Metrologia "G. Colonnetti". Il segnale degli orologi è diffuso con diverse tecniche, evolute nel tempo. Certamente è noto il segnale radiotelevisivo attraverso la RAI, così come la trasmissione attraverso sia la rete dati (Network Time Protocol, NTP) che con l'uso dei segnali satellitari, in particolare il GPS.

La sincronizzazione di un orologio remoto con il GPS è uno dei metodi più diffusi, tuttavia, per trasferire l'accuratezza di un orologio atomico di un istituto primario, sono necessari più di venti giorni di misura. Oggi la migliore realizzazione del secondo è data dagli orologi a fontana di Cesio, di cui esistono una decina di esemplari nel mondo (due all'INRIM). L'accuratezza di una fontana di Cs è di ~2×10-16 (frequenza relativa): le più sofisticate tecniche satellitari raggiungono questo livello in 20-40 giorni. Nel 2012, il premio Nobel della Fisica è stato attribuito a David Wineland per le sue ricerche sugli "orologi ottici", una nuova generazione di orologi atomici basati non più su una microonda, come nel caso del Cesio, bensì su radiazione visibile dello spettro elettromagnetico. Dal 2014, gli orologi ottici hanno consolidato un'accuratezza inferiore a 10-17, fino a 2×10-18, e sono basati su diversi atomi, come Yb, Sr, Hg, sia neutri che ioni. In Italia, per esempio, l'INRIM ha sviluppato un orologio ottico ad atomi neutri di Ytterbio.

Questi risultati aprono la strada a una ridefinizione del secondo rispetto all'attuale basata sulla transizione del Cesio a 9,19263177 GHz. Ancora molti passi si devono compiere prima di una ridefinizione, ma il processo è cominciato, esistendone il fondamento scientifico e tecnologico. Uno dei limiti attuali è il metodo di confronto remoto: per gli orologi ottici, i confronti satellitari richiedono fino a 1000 giorni di misura, chiaramente una situazione non adeguata.
Per risolvere il problema, dal 2005 è stata intrapresa la ricerca sul trasferimento in fibra ottica di segnali di laser ultrastabili in frequenza.

La tecnica si è consolidata in questi dieci anni dimostrando di essere adeguata alle prestazioni dei nuovi orologi. In particolare, a oggi sia in Germania che in Italia, su più di 1000 km di fibra è stato trasferito un segnale con incertezza aggiunta di ~1×10-19 in soli 1000 s di misura: valori adeguati a confrontare e distribuire anche gli orologi ottici. Del resto, questo sviluppo rivoluzionario ha un impatto generale nella metrologia di tempo, perché ora si può trasferire anche l'accuratezza degli orologi al Cs in tempi molto più brevi, non limitati dal sistema di sincronizzazione, ma dalla capacità degli orologi.

2. Come si può trasferire l'unità di tempo con un laser?

Un laser è una radiazione elettromagnetica di

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

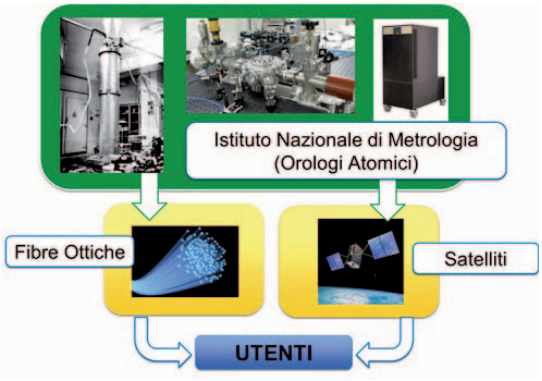


Fig 1 - I segnali degli orologi dell'INRIM - in alto, da sinistra: fontana criogenica al Cesio (Foto F. Bucciarelli), orologio a Ytterbio, Maser all'Idrogeno - possono essere distribuiti agli utenti tramite satellite e tramite fibra ottica.

frequenza definita: possiamo immaginare di mandarla in fibra affinché sia un oscillatore di trasferimento. La sua frequenza, misurata rispetto agli orologi dell'Istituto metrologico, arriva al laboratorio remoto e diventa un riferimento con il quale sincronizzarsi. Usando le fibre, la lunghezza d'onda del laser è scelta intorno ai 1550 nm. Per trasferire l'accuratezza, occorre un laser ultrastabile, ovvero con frequenza che non muti nel tempo, almeno di parti in 10-15 nel breve termine (1 s – 10 s). Pertanto, si usano tecniche di aggancio di fase del laser a cavità Fabry-Perot la cui lunghezza non cambia a quei livelli.

Un ostacolo è la fibra stessa, o meglio le variazioni della sua lunghezza per fattori ambientali di natura meccanica, termica o vibrazionale. La variazione di lunghezza della fibra si traduce sul laser in un rumore di fase, che deteriora le sue caratteristiche di stabilità, impedendo per esempio che l'incertezza si possa ridurre continuando a misurare. Per ovviare al problema, si applica una cancellazione attiva del rumore della fibra: una parte della radiazione a destinazione è retroriflessa verso il laboratorio di partenza. Qui ritornato, il segnale laser è confrontato con l'originale, da cui si ricava un'informazione sul rumore introdotto dalla fibra. Un attuatore optoelettronico compensa il rumore applicando una correzione uguale e contraria. E' solo con la cancellazione che si ottengono i risultati attesi, garantendo su più di 1000 km un contributo d'incertezza dalla fibra inferiore a 10-19 in 1000 s di misura. Affinché però la correzione sia efficace, la radiazione riflessa deve ripercorrere la stessa fibra, ovvero il cammino deve essere completamente bidirezionale, ponendo richieste di tipo infrastrutturale e strumentale. Infatti, occorre sia una fibra bidirezionale, e non il solito doppietto in fibra, che sistemi di amplificazione bidirezionali che non inneschino oscillazioni laser problematiche causate dalle riflessioni della fibra (in genere questo limita il gain degli amplificatori). Il link ottico è stato dimostrato sia in sistemi a fibra dedicata, o dark fiber, che in architettura WDM (Dense e Coarse), con un singolo canale dedicato in copresenza di altri utenti (i.e. traffico dati).

3. Il tempo in fibra in Italia e in Europa

In Italia, l'INRIM ha realizzato finora tre link ottici che collegano Torino al Tunnel del Frejus, a Medicina (Bologna) e a Sesto Fiorentino (Firenze). Questi 800 km di fibra costituiscono il primo segmento di una rete che si estenderà più a Sud, a Roma, Napoli e Matera tra il 2015 e il 2016, e si allaccerà a Nord alla rete europea di link fibra per il tempo a cui l'INRIM sta attivamente lavorando con i partner di Francia, Germania, UK e con gli organi della Metrologia Internazionale.

Sul tratto Torino-Firenze è stato realizzato anche un doppio link, che ha permesso di caratterizzare l'equivalente di 1300 km di fibra. Inoltre, dopo la sperimentazione iniziale, le tecnologie sviluppate sono mature per l'applicazione anche in ambito industriale.

La realizzazione dei collegamenti è avvenuta in collaborazione con il Consortium GARR, e per la parte verso il tunnel, ci si è avvalsi anche del Consorzio TOP-IX. Il link principale, tra Torino e il Polo Scientifico di Sesto Fiorentino (Università di Firenze, LENS, CNR), consente oggi di studiare proprietà della materia allo stato ultra freddo indagando le proprietà spettroscopiche più fini; tra gli esperimenti in corso ci sono diverse misure di fisica atomica e molecolare: fornendo il riferimento degli orologi attraverso la fibra si vuole misurare con sempre maggiore precisione i livelli energetici dei sistemi quantistici per indagare, per esempio, la stabilità temporale di alcune costanti fisiche fondamentali, messa in causa dalle teorie oltre il "Modello Standard".

Il secondo link ottico collega l'INRIM a Me-

dicina presso i radiotelescopi dell'INAF-IRA. I radiotelescopi sono dotati di orologi atomici commerciali sofisticati, i maser all'idrogeno, fondamentali per le osservazioni e per le tecniche di VLBI. L'uso del link ottico ha permesso di caratterizzare metrologicamente l'orologio posto a Medicina, e ora permetterà di studiare come il miglioramento del riferimento di frequenza possa beneficiare la risoluzione delle osservazioni radioastronomiche.

Il terzo link verso il tunnel del Frejus permetterà di confrontare, a un livello finora mai sperimentato, due orologi posti a una quota molto diversa (la differenza è di 1000 m), osservando così a quel livello d'incertezza gli effetti della relatività generale, che creano una differenza di frequenza tra orologi posti a potenziali di gravità diversa. Si parla per questi esperimenti di "geodesia relativistica", un campo ancora da esplorare, soprattutto considerando gli effetti dinamici del potenziale gravitazionale.

Per concludere, l'estensione verso Matera è motivata dalla convergenza di interessi di geodesia e di radioastronomia, essendoci in Matera il Centro di Geodesia Spaziale dell'ASI, che si avvale di antenne radioastronomiche pilotate da orologi al maser di idrogeno. In questo caso, migliorare l'accuratezza del riferimento tramite l'estensione del link ottico Torino-Matera vuole migliorare il livello di precisione della geodesia per avere un monitoraggio più fine degli effetti geofisici che riguardano il pianeta.

Fig 2 - Una rete europea di link ottici grazie alla collaborazione tra le reti della ricerca.

A questa attività italiana si accompagna un intenso sforzo per realizzare una rete europea di link ottici, a cominciare dai collegamenti dei primi quattro istituti metrologici, che si trovano in Francia, Germania, Italia e UK. Questi link consentiranno un confronto diretto degli orologi ottici di questi istituti, un passo importante verso la ridefinizione del secondo. Da questi collegamenti fondamentali, poi, si potrà ampliare verso i centri scientifici di eccellenza, le comunità scientifiche più coinvolte (es. la geodesia spaziale) e infine l'industria continentale.

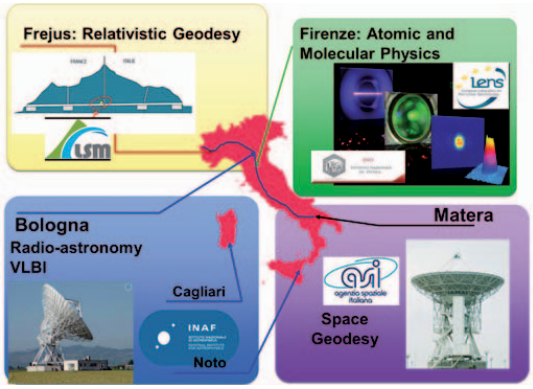


Fig 3 - La trasmissione del secondo in ambito multidisciplinare

La rete in fibra, oltre a trasportare dati, si avvia sempre più a portare un riferimento di tempo ultra-preciso, su cui si potrà costruire una parte del futuro scientifico e tecnologico europeo.

Collaborano al progetto del link ottico

E. Bertacco, C. Calosso, C. Clivati, M. Frittelli, F. Levi, G. A. Costanzo.

Il Link Ottico dell'INRIM è stato realizzato con il sostegno della Compagnia di San Paolo e del MIUR (programma "Progetti premiali").

Riferimenti bibliografici

D. Calonico, R. Oldani, Il tempo è atomico. Breve storia della misura del tempo, Hoepli Editore, p. 250, 2013.

Davide Calonico
d.calonico@inrim.it
Ricercatore all'INRIM, divisione di Metrologia Fisica, dove lavora alla realizzazione di orologi atomici a fontana di Cesio (che realizzano l'unità di tempo), e a Ytterbio in reticolo. Da alcuni anni contribuisce allo sviluppo della distribuzione in fibra dei segnali campione.

Soluzioni per la posta elettronica in un Ateneo di medie dimensioni

Roberta Cantaroni

Università di Modena e Reggio Emilia

Abstract. Il servizio di posta elettronica all'interno dell'Università degli studi di Modena e Reggio Emilia è attualmente realizzato con una soluzione ibrida e 2 domini separati. Il dominio @unimore.it, dedicato a personale docente e tecnico-amministrativo, collaboratori esterni, strutture e uffici (3200 mailbox e 8000 indirizzi/alias) è gestito interamente con una soluzione in-house realizzata su infrastruttura VMware e software prevalentemente OpenSource. Il dominio @studenti.unimore.it, dedicato a studenti e dottorandi (40.000 mailbox/indirizzi di studenti attivi e alum), è gestito dal 2008 su piattaforma Google Apps Education.

1. Introduzione

L'Università degli Studi di Modena e Reggio Emilia è un ateneo a reti di sedi (Modena e Reggio Emilia) con 14 Dipartimenti, 19 Centri di Servizio e di Ricerca, 7 Direzioni Operative, circa 1.500 unità di personale e 20.000 studenti. Il sistema di posta elettronica è centralizzato dal 2001 e gestito da due tecnici dedicati. Per la gestione degli indirizzi di posta istituzionali è stata adottata una soluzione ibrida che prevede la gestione di 2 domini separati: @unimore.it, dedicato al personale docente, tecnico-amministrativo, collaboratori esterni, strutture e uffici gestito con una soluzione realizzata interamente in-house e @studenti.unimore.it, dedicato a studenti e dottorandi gestito su piattaforma Google Apps Education. Mailbox e indirizzi seguono il ciclo di vita dell'incarico istituzionale di ciascun utente e sono attivati/disattivati/riattivati in tempo reale in base ai dati presenti nel repository LDAP di Ateneo. Gli indirizzi istituzionali sono iscritti a liste di distribuzione per ruolo/struttura/Dipartimento. Le mailbox devono essere usufruibili 24/24h, da qualunque client di posta interno ed esterno, all'istituzione tramite canali sicuri POPS/IMAPS/HTTPS e devono essere il più possibile libere da spam e virus. L'accesso avviene con le credenziali unificate assegnate all'utente per l'accesso a tutti i servizi Unimore. Nel caso del personale è sentita l'esigenza di recuperare agevolmente messaggi cancellati per errore.

2. Il servizio @unimore.it in-house

Per ragioni di sicurezza, privacy e riservatezza dei dati, il servizio è gestito al momento interamente in-house [1]. I nodi di elaborazione sono raggruppati per la maggior parte su un unico cluster di virtualizzazione VMware che ospita quasi tutti i servizi amministrativi e centralizzati dell'Ateneo (autorizzazione/autenticazione, condivisione files, web, posta, etc) e fornisce infrastruttura di elaborazione ai Dipartimenti, alle strutture dell'Ateneo e a strutture esterne convenzionate.

L'infrastruttura sistemistica, concentrata nella sede di Modena, si basa su uno chassis Blade Server con 16 nodi di elaborazione, collegati con tecnologie di datacenter bridging (Fabric Fiber Channel ed Ethernet Fabric) ad un apparato SAN storage multiprotocollo e 4 storage NAS con una capacità totale di 100 Tb, 1 Tb di RAM e 300GHz di risorse CPU. Il servizio di posta elettronica @unimore.it occupa attualmente in totale circa 7 Tb.

I componenti del servizio sono stati separati logicamente per tipologia e realizzati con software prevalentemente OpenSource scegliendo soluzioni che garantiscano alta affidabilità. I log dei vari componenti sono centralizzati mediante rsyslogd.
Il servizio gestisce attualmente 3200 mailbox e 8000 indirizzi/alias (*fig.1*), conta in media 2.000 accessi distinti POPS/IMAPS al giorno, 400.000 messaggi spediti al mese, 50.000 messaggi/giorno da fuori dominio con oltre il 95% di email di spam individuate e bloccate e più di 400 liste di distribuzione e di discussione. Gli indirizzi nominali sono assegnati nella forma nome.cognome@unimore.it

2.1 MX di dominio

Gli MX di dominio sono realizzati con 4 VM su piattaforma VMware, sistema operativo Debian

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

Componente	Hardware	Servizi	Software
MX (Mail eXchanger) di dominio	4 VM	Antivirus/Antispam	Sophos PureMessage
Posta in arrivo	Cluster 2 server fisici + 1 VM	POPS/IMAPS e autenticazione su LDAP	CentOS Cluster Suite, Dovecot, Postfix
Spedizione via SMTP	4 VM	SMTPS con autenticazione su LDAP	Exim4, SpamAssassin, Clamd
Liste di distribuzione per ruolo/struttura	1 VM	Spedizione limitata a indirizzi @unimore.it con controllo d'identità /Aggiornamento giornaliero degli iscritti con LDAP	Sympa
Liste di discussione	1 VM	Amministrazione via web da parte dei proprietari	Mailman
Backup/Restore email	1 VM	Recupero email da interfaccia web	Zimbra
Sistema di monitoraggio	1 VM	Controllo costante dei servizi attivi sui nodi	Munin

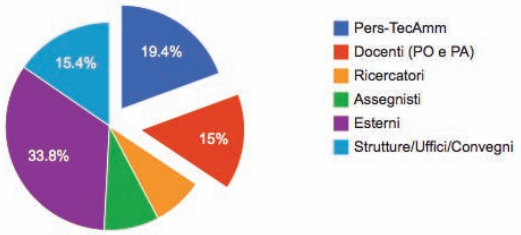


Fig. 1 Distribuzione degli indirizzi @unimore.it

wheezy, 4 Gb RAM, file system di tipo xfs, 80 Gb per software antispam/antivirus e database della quarantena. Il carico è distribuito mediante sistema round robin del DNS con uguale priorità. Gli MX ricevono la posta dall'esterno del dominio e la consegnano al server della posta in arrivo dopo i controlli antivirus e antispam realizzati con software proprietario (Sophos PureMessage [2]) e filtri a livello MTA Postfix (check_recipient_access, reject_non_fqdn_helo_hostname, reject_unknown_sender_domain, reject_non_fqdn_sender, reject_unverified_sender, …).

Ogni VM mantiene una coda locale di email in modo che un eventuale fermo del servizio MTA implichi un ritardo solo nella consegna dei messaggi in quella coda. Per policy le email riconosciute spam (probabilità > 50%) sono bloccate nello spazio di quarantena, condiviso tra i 4 server, per 5 giorni. Ogni utente può autorizzare il mittente richiedendo la consegna in caso di falso positivo, bloccare un mittente "fastidioso" e richiedere la consegna di un digest giornaliero con le intestazioni delle email bloccate.

2.2 Posta in arrivo

Il servizio che gestisce la memorizzazione della posta in arrivo e l'accesso POPS/IMAPS è quello più critico perchè un suo disservizio viene immediatamente avvertito da tutti i client che accedono in quel momento. È stato realizzato su un cluster di tre nodi (2 fisici e 1 VM) con software di clusterizzazione Cluster Suite di CentOS 6, 16 Gb RAM, software OpenSource (*fig.2*). I tre nodi condividono una LUN dedicata su SAN VMware con file system di tipo xfs, 3 Tb di storage per le mailbox (occupazione attuale 55%). Sullo storage è attivo il Tiering automatico (1.63% extreme performance (SSD), 70.02% performance (SAS), 28.35% performance (nSAS). Un solo nodo è attivo in ogni momento ed eroga i servizi di cluster (filesystem, IP a cui corrisponde il record A mail.unimore.it, Mysql, Dovecot, Postfix, httpd). Sul filesystem risiedono i messaggi, il database con mailbox e indirizzi, la coda di posta, gli script per la gestione (creazione/cancellazione/disattivazione) e l'interfaccia web che consente attivazione di vacation/forward e ricerca indirizzi. Ogni mailbox ha una quota personalizzata (default 500 Mb), il formato è Maildir, la dimensione massima dei messaggi (testo + attachment) è di 25 Mb.

L'accesso è realizzato tramite replica locale del sistema LDAP di Ateneo attiva sui 3 nodi. La logica del cluster prevede che i nodi si "sentano" tra-

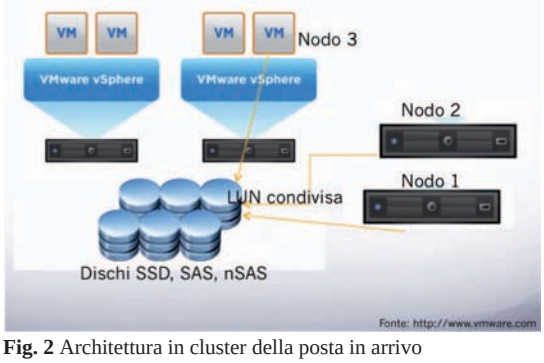


Fig. 2 Architettura in cluster della posta in arrivo

mite dati scritti su quorum disk e che i servizi di cluster migrino su uno degli altri nodi in caso di disservizio su quello attivo. La soluzione adottata è scalabile, consente il riavvio rapido dei servizi in caso di failure su un nodo, consente clone e snapshot periodici sia del nodo realizzato su VM che dello storage e consente la migrazione dei servizi dal nodo attivo ad altro nodo in caso di operazioni di aggiornamento o manutenzione.

2.3 Spedizione via SMTP

Il servizio SMTP permette la spedizione con autenticazione TLS e le stesse credenziali della posta in arrivo. Consegna al server della posta in arrivo nel caso di destinatari @unimore.it ed è abilitato alla consegna all'esterno di Unimore. È realizzato con 4 VM su piattaforma VMware, con sistema operativo Debian wheezy, 2 Gb RAM, 10 Gb storage, file system di tipo xfs. Il nome è unico (smtp.unimore.it) e ad esso corrispondono 4 record A nel DNS, il carico è distribuito mediante sistema round robin del DNS.

Le email spedite sono controllate da antivirus e antispam realizzati con software OpenSource (Clamd, SpamAssassin) e filtri a livello MTA (Exim4) in grado di bloccare l'invio con credenziali compromesse e/o limitare il numero di email spedite all'ora per username. Ogni VM mantiene una coda locale di email, un eventuale fermo del servizio MTA implica un ritardo solo nella consegna dei messaggi in quella coda.

2.4 Liste di distribuzione e di discussione

Le liste di distribuzione per struttura e ruolo sono circa 250 e sono gestite con il software OpenSource Sympa [3]. La spedizione è limitata agli indirizzi @unimore.it mediante controllo di identità. L'elenco degli iscritti è ottenuto con filtri sugli indirizzi degli utenti attivi in LDAP. La consegna dei messaggi alle liste numerose è effettuata utilizzando la modalità hard link di Dovecot (comando dovecot-lda con opzione –p [4]) ottenendo in questo modo un notevole risparmio di spazio disco dato che l'invio ad una lista di N indirizzi equivale alla memorizzazione su disco del singolo messaggio. Sono inoltre attive circa 150 liste di discussione gestite con il software OpenSource Mailman [5]. Gli amministratori delle liste possono accedere via interfaccia web alla configurazione delle liste, alle iscrizioni e alla moderazione dei messaggi.

2.5 Backup e restore

Per gestire il disaster recovery, ma anche per consentire il rapido recupero di messaggi cancellati per errore dagli utenti, sono attivi diversi sistemi paralleli di backup:

- snapshot periodici schedulati sulla SAN (1/gg con retention di 7gg);
- sincronizzazione settimanale del contenuto dello spazio mailbox su storage parallelo mediante rsync e ripristino su richiesta di messaggi o folder;
- copia in tempo reale su altro server di posta (realizzata mediante l'opzione recipient_bcc di Postfix) dei messaggi ricevuti sugli indirizzi istituzionali.

Il server di posta è basato su Zimbra Collaboration OpenSource Edition installato su una VM con Centos 6, 4 Gb RAM, 800 Gb storage e consente agli utenti di accedere via webmail al recupero di messaggi ricevuti e cancellati per errore negli ultimi 3 mesi.

2.6 Sistema di monitoraggio

Su ogni server è installato il software OpenSource Munin, componente "node", che consente di monitorare non solo il carico in termini di cpu, memoria e spazio disco, ma anche la coda di email e di avvisare con warning e alert in caso di superamento delle soglie impostate. La configurazione dei servizi e delle soglie è gestita con Munin, componente "master", installato su una VM dedicata. Il controllo e il riavvio automatico dei processi critici è gestito mediante il software OpenSource Monit.

3. Il servizio @studenti.unimore.it su Google Apps Education

Ogni studente, all'atto dell'immatricolazione, riceve un indirizzo nel formato <ID>@studenti.unimore.it, dove ID è l'identificativo assegnato dalle Segreterie Studenti. I dottorandi ricevono anche l'alias nel formato nome.cognome@unimore.it che possono impostare nel campo From.

L'indirizzo rimane attivo per 3 anni dopo il conseguimento del titolo (stato di alumn).

Dal 2008 il dominio studenti.unimore.it è gestito su piattaforma Google Apps Education. I servizi attivati sono Posta, Calendar, Drive e Chat. L'interfaccia web non presenta banner pubblicitari [6]. L'autenticazione via webmail avviene me-

diante Shibboleth con le credenziali centralizzate Unimore. Per mantenere la tracciabilità dei log, le email ricevute e spedite passano dai server MX e SMTP di Unimore. I limiti attuali sono quelli impostati da Google: spazio "illimitato", dimensione massima dei messaggi (testo + attachment) 25 Mb. Per ogni studente, i dati inviati ai server di Google sono soltanto username, nome, cognome e una password secondaria utilizzata dallo studente per accedere via client di posta. Si richiede che questa password sia mantenuta diversa da quella centralizzata Unimore.

Il servizio gestisce attualmente circa 40.000 mailbox/indirizzi attivi (studenti + alumni) con una media di 15.000 accessi distinti al mese e 500.000 email spedite/mese. Sono attivi 17 gruppi Google sincronizzati giornalmente con LDAP (tutti gli studenti attivi, gli alum, i dottorandi, gli studenti suddivisi per Dipartimento) a cui corrispondono 17 liste di distribuzione utilizzate da personale e uffici per le comunicazioni con gli studenti previo controllo di identità. Le procedure di aggiornamento dei gruppi sono state realizzate con script Ruby e Google Admin SDK.

4. Ciclo di vita di mailbox e indirizzi

Un utente ha diritto all'accesso ai servizi Unimore per tutto il periodo di durata dell'incarico a lui assegnato. Un applicativo denominato "correlatore" (*fig. 3*) si preoccupa di sincronizzare il sistema LDAP di Ateneo con i dati provenienti da 3 distinte banche dati: quella del personale, quella degli studenti e quella dei collaboratori esterni.

Per la gestione del ciclo di vita di mailbox e indirizzi è utilizzato il sistema di messaggistica Apache ActiveMQ. I sistemi POSTA ed LDAP sono entrambi producer e consumer di messaggi. Nel caso degli indirizzi @unimore.it:

- ogni variazione su LDAP (utenti aggiunti, utenti cancellati, account che cambiano utente di riferimento) invia un messaggio ad una coda a cui segue l'azione corrispondente nel sistema POSTA @unimore.it (creazione/riattivazione/disattivazione di mailbox e indirizzi) realizzata mediante script Ruby;
- ogni nuovo indirizzo attivato è segnalato con un messaggio su una coda letta da LDAP che si preoccupa di riempire il campo unimoreMail dell'entry utente.

Nel caso degli indirizzi @studenti.unimore.it:

- ogni variazione su LDAP (studenti aggiunti, studenti cessati, studenti che cambiano organizational unit (ou) cioè che diventano alumn o passano da studente a dottorando o da registered a studente) genera un messaggio ad una coda a cui segue l'azione corrispondente nel sistema POSTA @studenti.unimore.it (creazione/riattivazione/disattivazione) realizzata mediante script Ruby e Google Admin SDK;
- ogni nuovo indirizzo attivato è segnalato con un messaggio su una coda letta da LDAP che si preoccupa di riempire il campo unimoreMail dell'entry studente.

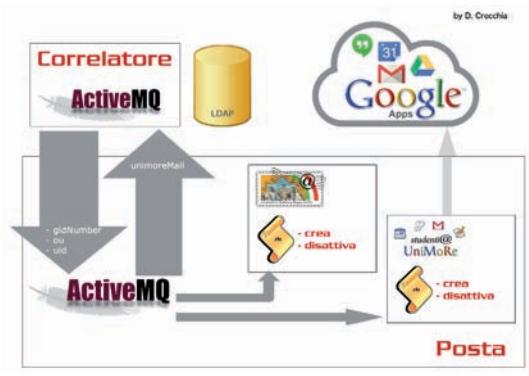
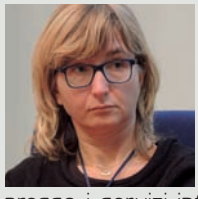


Fig. 3 Gestione del ciclo di vita di mailbox e indirizzi

Riferimenti bibliografici

[[1] Portale dei servizi di posta elettronica @unimore.it http://posta.unimore.it
[2] http://www.sophos.com
[3] Portale liste di distribuzione Unimore http://circolari.unimore.it
[4] http://wiki.dovecot.org/LDA
[5] Portale liste di discussione Unimore http://liste.mail.unimo.it
[6] Portale dei servizi di posta elettronica @studenti.unimore.it http://start.studenti.unimore.it



Roberta Cantaroni
roberta.cantaroni@unimore.it

Laureata in Matematica nel 1987. Lavora dal 1990 come personale tecnico presso i servizi informatici (rete, fonia e sistemi) dell'Università degli studi di Modena e Reggio Emilia. Gestisce il servizio di posta elettronica e l'infrastruttura per il rilascio di PEC e firma digitale.

Progetto EduNet

Marco D'Ambrosio

Università di Cassino e del Lazio Meridionale

Abstract. Il progetto EduNet è nato dall'idea di collegare gli Istituti scolastici a GARR tramite la rete in fibra ottica UnicasNet, di proprietà dell'Università di Cassino e del Lazio Meridionale.
EduNet si propone di riuscire a rendere disponibile la tecnologia comunemente utilizzata dai centri di ricerca, mediamente più avanzata di almeno 10 anni, già a partire dalle scuole dell'infanzia.
Il compito dell'Università in questo processo è quello di supporto per il Dirigente Scolastico, orientandolo verso le scelte che riteniamo essere corrette, aiutandolo ad accelerare l'innovazione nella didattica e a favorire la sperimentazione, portando la ricerca universitaria nelle scuole.
Ogni Istituto avrà il compito di autofinanziare l'allaccio a UnicasNet/GARR, sotto la supervisione e l'esperienza dell'Università. I veri protagonisti di EduNet sono i servizi e le applicazioni, tra cui il BYOD (bring your own device) integrato con la federazione Eduroam, LOLA (Low Latency audio visual streaming system) e molto altro.

1. Introduzione

Il progetto EduNet è nato inizialmente dall'idea di collegare gli Istituti scolastici a GARR tramite la rete in fibra ottica UnicasNet, di proprietà dell'Università di Cassino e del Lazio Meridionale. In corso d'opera EduNet, però, si è trasformato in una sorta di movimento culturale agente sul territorio della Provincia di Frosinone, che mira a rivoluzionare il sistema educativo partendo da iniziative innovative, di tipo collaborativo, molto spesso promosse da volontari

2. Il Progetto

EduNet si propone di riuscire a rendere disponibile la tecnologia comunemente utilizzata dai centri di ricerca, mediamente più avanzata di almeno 10 anni, già a partire dalle scuole dell'infanzia, rispettando il motto "Insegnare ad utilizzare nel presente gli strumenti del futuro". Questo è possibile grazie a scelte corrette in ambito tecnologico, ad un utilizzo virtuoso delle risorse disponibili e ad un approccio più "social", che privilegi la collaborazione tra più soggetti.

Figura centrale del progetto è il Dirigente Scolastico, che diventa il vero regista di questo processo di trasformazione, poiché agisce da collettore comunicativo ideale tra Università, GARR, produttori, fornitori, finanziatori e consulenti. Il compito dell'Università in questo processo è quello di guida per il Dirigente Scolastico, aiutandolo ad accelerare l'innovazione nella didattica e a favorire la sperimentazione, portando la ricerca universitaria nelle scuole. Altro importante ruolo dell'Università è quello di dare corrette informazioni sull'opportunità di far parte della "Comunità GARR", descrivendo i servizi disponibili e mettendo a disposizione il know-how acquisito nel corso degli anni.

Fig. 1 Logo del progetto EduNet

Recentemente, al coro degli "evangelizzatori" delle tecnologie avanzate per le scuole, si sono aggiunti anche alcuni sindaci e amministratori locali che, capita l'importanza e le potenzialità di tale investimento, dal breve al lungo termine, sono diventati portavoce di EduNet, spesso mettendo in campo risorse economiche e la non trascurabile disponibilità delle infrastrutture territoriali per agevolare e rendere meno onerosa la posa di fibra ottica; tale attività può essere svolta sia dagli operatori di telecomunicazioni, sia di-

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

rettamente dagli enti pubblici, scuole comprese. Per quest'ultimo caso ci sono almeno 3 esempi, tra cui si evidenzia l'encomiabile sforzo dell'I-IS Einaudi-Baronio di Sora (FR), che ha realizzato ex-novo un'infrastruttura di proprietà, lunga 1,5 km, che si estende nel centro di Sora ed è composta da un cavo a 24 fibre ottiche che collega ad UnicasNet/GARR i loro due plessi.

La connettività è il primo punto dal quale partire, che deve essere "capace" a sufficienza, simmetrica, deve crescere con le esigenze degli utenti ed essere considerata sempre un'opportunità di crescita, mai vista come un limite.

La novità principale di questo modello è che ogni Istituto avrà il compito di autofinanziare l'allaccio a UnicasNet/GARR, sotto la supervisione e l'esperienza dell'Università. Come con le costruzioni "lego", ognuno costruirà la propria micro-rete. UnicasNet fungerà da aggregatore e "armonizzatore" territoriale, GARR farà altrettanto a livello nazionale e internazionale. GARR, quindi, è la ragion d'essere e il principale valore intrinseco di EduNet, poiché ne amplifica il valore e proietta UnicasNet e i suoi utenti, in modo efficiente, nel mondo delle reti della ricerca ad alte prestazioni.

Passando agli aspetti tecnici, lo schema logico di connessione degli utenti di EduNet prevede la costituzione di una nuvola layer2 sulla quale insistono i router di terminazione, presenti nella sede dell'utente, con velocità di accesso da 100Mbps simmetrici a 10Gbps simmetrici.

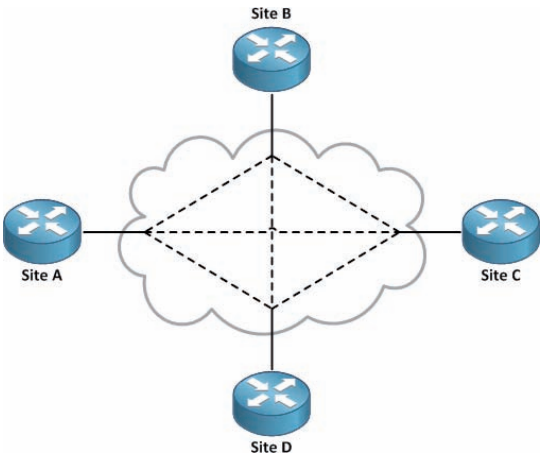


Fig. 2 Schema logico di connessione degli utenti di EduNet

Le subnet pubbliche IPv4 e IPv6 assegnate agli utenti sono annunciate agli altri router tramite OSPF, massimizzando quindi l'efficienza nelle connessioni tra gli istituti, senza impattare sul router GARR di frontiera. È possibile attivare path layer2 diretti o addirittura path ottici diretti (limitatamente alle sedi collegate in fibra ottica) per la sperimentazione di applicazioni speciali (es. LOLA) che non sempre risultano adeguatamente veicolabili dai router tradizionali.

Altro elemento di distinzione è l'uso massiccio della tecnica della "passive inspection" per il logging del traffico, rendendo di fatto inutili i firewall tradizionali configurati in modalità attiva. Con questa tecnica è possibile monitorare grandissime quantità di traffico con hardware di commodity e software opensource. Inoltre, grazie alla responsabilizzazione personale del traffico (ovvero ogni pacchetto ha sempre un nome e cognome, con tale informazione memorizzata nelle sedi dei singoli utenti per 6 mesi) è possibile ridurre, se non del tutto eliminare come hanno deciso in molti, il meccanismo di content filtering. Sempre tramite "passive inspection" è possibile attivare meccanismi di IDS (Intrusion Detection System), in grado di segnalare in modo tempestivo (ad esempio via email o agendo direttamente, nei casi più gravi, sulle access list del router) eventuali host infetti in grado di creare danni alla rete. Gli host in questione dovranno essere prontamente bonificati, non semplicemente arginati come normalmente avviene.

Non tutti hanno apprezzato e accettato inizialmente questo radicale cambiamento di rotta, ma i Dirigenti Scolastici che hanno deciso di compiere coraggiosamente tale passo hanno immediatamente raccolto riscontri positivi, sia dall'utenza che sullo stato di sicurezza generale della rete, soprattutto per ciò che riguarda la gestione degli incidenti di rete, in collaborazione con GARR.

È un po' come scegliere tra l'avere una rete assimilabile ad un carcere con dentro rinchiusi delinquenti, che hanno una libertà molto limitata e che comunque non possono nuocere all'esterno, piuttosto che avere un residence composto principalmente da persone per bene, libere di muoversi, dove è presente un servizio d'ordine e di sicurezza che interviene so-

lo in caso di necessità.

Sebbene l'aspetto tecnologico e topologico sia importante da descrivere e analizzare, essendo tra l'altro fortemente influenzato dall'idea di incentivare la collaborazione attiva tra gli Istituti connessi, risulta visto dall'alto come uno degli aspetti meno evidenti dell'intero progetto. L'obiettivo infatti è quello di rendere così veloce ed efficiente la rete da essere percepita come del tutto "trasparente" all'utente finale.

Le vere protagoniste di EduNet sono, infatti, i servizi e le applicazioni. Si parte con la diffusione massiccia del BYOD (bring your own device) in ogni Istituto, realizzato a regola d'arte e in grado di sopportare il carico di tutti i dispositivi di rete che "vivono" nella scuola, senza limitazione alcuna, ma prevedendo la responsabilizzazione e tracciabilità delle attività del singolo individuo, rispettando allo stesso tempo la normativa vigente sulla privacy. Anche questa è una forma di educazione e preparazione al mondo reale, che deve avvenire (a nostro avviso) senza filtri, costrizioni o negazioni, seppur sotto la insostituibile guida dei docenti.

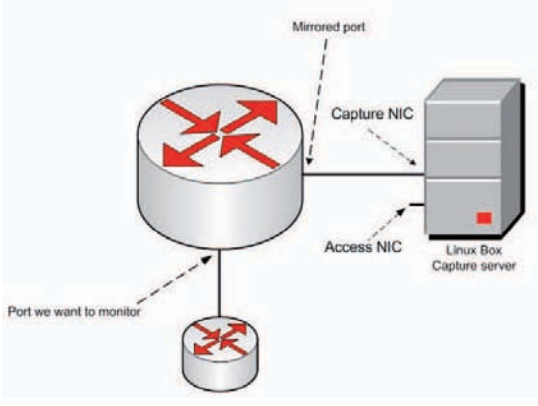


Fig. 4 Passive inspection per il logging del traffico

D'altra parte lo stesso accesso a GARR è completamente trasparente, sia in termini di protocolli di comunicazione che di contenuti; per quale motivo le cose dovrebbero funzionare diversamente per l'utente finale?

L'accesso alla federazione Eduroam è un elemento che amplifica notevolmente la tecnica del BYOD, estendendone la sua efficacia anche in mobilità, addirittura a livello globale. Bisogna aiutare gli Istituti ad attivare questo servizio, sebbene dipenda strettamente dalla presenza di una infrastruttura adeguata. Recentemente, rispetto al passato, è aumentata sensibilmente la disponibilità di hardware e software in grado di creare infrastrutture Wi-Fi capaci di connettere in modo efficiente un gran numero di utenti e in grado di fronteggiare l'eventuale presenza di interferenze. Ovviamente bisogna garantire sempre il massimo rispetto delle raccomandazioni ministeriali circa le emissioni in radiofrequenza, nonché tenere presente che per alcune applicazioni è necessario ricorrere alle prestazioni (in termini di banda, latenza, jitter e packet loss) che solo un collegamento via cavo può garantire (es. LOLA).

La cosa che ha molto sorpreso è che, in Italia, le prime adesioni delle scuole ad Eduroam siano nate proprio nel nostro territorio, grazie all'Università di Cassino e del Lazio Meridionale; il motivo è che le scuole, anche quelle già connesse a GARR da molto tempo, hanno semplicemente bisogno di aiuto; una volta attivato il servizio non manca occasione per apprezzarne l'utilità.

EduNet, inoltre, ha dimostrato che il "divide" sul know-how dei docenti, circa l'utilizzo dei moderni strumenti tecnologici, può essere facilmente superato invertendo per un attimo i ruoli e utilizzando le competenze degli studenti più brillanti. È importante citare, a tal proposito, l'esperienza vissuta dal Liceo di Ceccano (FR) il 2 settembre 2014, giornata in cui sono stati gli studenti ad aver insegnato ai propri docenti l'uso dei moderni strumenti di condivisione delle risorse e di informazioni sulla rete.

L'obiettivo finale è quello poi di aiutare i docenti ad anticipare, e non inseguire, i ragazzi nell'uso delle moderne tecnologie, evitando di demonizzare strumenti, al contrario, utilissimi per la didattica. Su questo l'Università e la ricerca possono svolgere un'azione fondamentale.
EduNet, come esempio di ricerca applicata all'istruzione, ha già iniziato ad applicare in contesti scolastici, per la prima volta, la tecnologia LOLA (Low Latency audio visual streaming system), applicazione ideata e realizzata dal Conservatorio di Trieste e da GARR.

Non finisce qui, EduNet va oltre il traffico IP

e tenta anche di illuminare le fibre in un modo inedito, ovvero veicolando segnali audio e video senza compressione su distanze fino a 80km, sfruttando la grande quantità di fibre ottiche ancora disponibili nell'infrastruttura UnicasNet. L'idea è quella di creare una rete ottica territoriale in alta definizione, per applicazioni di teledidattica e telepresenza, fino a creare un centro di produzione audiovisiva. Tale rete sarà estesa anche alle scuole che decideranno di allacciarsi in fibra ottica spenta.

Ancora, EduNet ha in mente di allargarsi verso progetti per la creazione di "smart cities", passando per attività sperimentali di "building automation" e cercando soluzioni avanzate per il risparmio energetico. Tali attività saranno sviluppate sia con la collaborazione dei centri ricerca interni all'Università, ma anche con l'aiuto esterno dei gruppi di volontari e appassionati, associazioni culturali, sindaci, amministratori locali, imprenditori e figure comunemente chiamate "technology evangelists".

Al momento le scuole connesse ad UnicasNet/GARR sono 8 (http://www.garr.it/a/scuole/utenti/scuole-collegate#LAZIO), ma l'Università di Cassino e del Lazio Merdionale è al lavoro con altre 20 scuole, con l'obiettivo di collegarle prima possibile.

Uno dei nostri desideri, sicuramente, è di veder replicato tale modello in altre zone dell'Italia, ove applicabile, nonché condividere esperienze e correggere insieme eventuali punti di debolezza riscontrabili. È, inoltre, auspicabile la creazione, in collaborazione con GARR, di whitebooks e aree informative sul web, dove condividere pubblicamente tutorial ed esperienze d'uso.

Marco D'Ambrosio
m.dambrosio@unicas.it

Appassionato di tecnologia e di musica.
Per il Centro di Ateneo per i Servizi Informatici, dell'Università di Cassino e del Lazio Meridionale, si occupa principalmente dei progetti sperimentali e di ricerca. Attualmente è impegnato nella diffusione sul territorio del progetto "EduNet", curandone gli aspetti progettuali e realizzativi.

Rischi per l'utente finale durante le connessioni a Wi-Fi pubbliche non cifrate

Andrea Lora

CNR-Istituto di Cristallografia - Area della Ricerca Roma 1

Abstract. Connettersi ad una rete wireless 802.11 non protetta espone il client finale ad alcuni attacchi. Alcuni di questi sono di tipo Denial of Service, altri, più complessi, sono finalizzati alla sottrazione di credenziali di accesso, all'acquisizione di dati personali o all'elusione delle tecnologie di sicurezza che la rete offre. Verranno analizzati alcuni di questi attacchi al fine di aumentare la consapevolezza sull'utilizzo delle Wi-Fi pubbliche concentrandosi in particolare sull'interazione Wi-Fi pubblica e captive portal di autenticazione.

1. Introduzione

L'implementazione attuale delle reti metropolitane e regionali Wi-Fi di tipo pubblico si basa su tecnologia di tipo 802.11 b/g/n ad accesso non protetto (assenza di crittografia WEP o WPA) con l'ausilio di Captive Portal per l'autenticazione. Il client si connette ad un SSID annunciato (ad es. provinciawifi), riceve un indirizzo IP dal DHCP locale, e viene messo in "client isolation". Successivamente qualsiasi richiesta di tipo HTTP prevede il reindirizzamento ad un Captive Portal che richiede le credenziali di accesso al sistema o la registrazione ad esso. Qualunque altra richiesta verso porta non standard viene silenziosamente scartata. A seguito di immissione di credenziali corrette l'IP del client viene sbloccato e viene consentito l'accesso verso internet. Questo tipo di approccio si presta ad una serie di attacchi, verranno dunque illustrati quelli che coinvolgono il client finale.

2.Attacchi DOS

Gli attacchi di tipo Denial of Service su questo tipo di rete sono quelli comuni a 802.11.

Il Wi-Fi Jamming prevede l'occupazione del canale radio dove opera l'AP che viene riempito (flooding) con traffico dati, limitando la capacità di fornire il servizio. A causa dell'utilizzo del protocollo CSMA/CA da parte di 802.11, i client o l'access point si vedrebbero deteriorare o completamente annullare le capacità di trasmissione. L'attacco può avvenire sia sul layer PHY che sul MAC.

Il DeAuth Attack invia pacchetti contraffatti (spoofed) che forzano il client a scollegarsi dall'access point. Le tecniche che comportano la perdita di connessione sono molteplici, ma tutte si basano sulla possibilità di un dispositivo terzo di inviare un pacchetto spoofed, spacciandosi per un altro dispositivo. Alcuni pacchetti di servizio, tipici di 802.11, sono in grado di disassociare o deautenticare il client dall'access point. Contraffacendo un pacchetto appositamente forgiato si è quindi in grado di ottenere la disconnessione. Sono stati proposti dei workaround a questo problema che non colpisce solo le reti non crittografate, ma anche quelle protette da WPA e WEP. I pacchetti di servizio nello standard 802.11, infatti, non si avvalgono mai di crittografia se non nel futuro standard 802.11w, che aggiungerà un valore di hash a tutti i frame di management.

L'Authentication Flood invia un elevato numero di richieste contraffatte di autenticazione verso l'access point, mirando all'esaurimento delle sue risorse. Potendo contare sullo spoofing dei pacchetti, un attaccante è in grado di generare centinaia di richieste di associazione all'access point che potrebbero andare a saturare la memoria del dispositivo, inibendo la possibilità di accettare nuove associazioni (nel migliore dei casi) o un suo malfunzionamento che impedisce di comunicare anche con i client già associati.
Il DHCP Starvation opera a layer più elevato, invia numerose richieste DHCP e tenta di esauri-

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

re il pool di IP assegnabili. La tecnologia di autenticazione con Captive Portal necessita che il client abbia uno stack IP completamente funzionante per potersi autenticare. Da qui la necessità che sulla rete ci sia un DHCP che assegna gli IP non appena la connessione è stabilita. Anche in questo caso l'attaccante può contare sullo spoofing e saturare una subnet /24 in pochissimo tempo. A seconda della topologia della rete questo attacco può ripercuotersi su Access Point fisicamente distanti da quello attaccato ma che ne condividono la rete.

2. Client Isolation

Una parte della sicurezza delle reti aperte è affidata alla capacità di alcuni Access Point che consentono di attivare il cosiddetto Client Isolation (il nome varia a seconda del vendor), una feature atta ad impedire lo scambio di dati tra client collegati allo stesso AP, di fatto inibendo la possibilità di stabilire le comunicazioni tra client. Ciò è possibile poiché le specifiche 802.11 prevedono che a seguito di una connessione ad una rete managed (non ad hoc) i client possano trasmettere e ricevere dati solamente con l'Access Point.

L'implementazione per raggiungere questo scopo consiste nell'inibire il trasporto di pacchetti che devono raggiungere il dominio di broadcast locale non aventi target mac address autorizzati. In una rete composta da un access point e due client l'ARP request inviata dal Client 1 per richiedere l'indirizzo Ethernet dell'IP a cui è associato il Client 2 viene silenziosamente scartata. Il Client 2 non riceverà mai la richiesta ARP e non potrà inviare dunque risposta. Anche in presenza di ARP table con entry statiche la client isolation continua a impedire la comunicazione tra i client. I client non sono mai consapevoli di essere in client isolation poiché è una feature dell'AP e gestita interamente da lui.

Considerato che il traffico tra il Client 1 e l'AP viaggia su etere è possibile per un attaccante intercettarlo e fingendosi l'AP, trasmettere l'informazione al Client 2, che a sua volta risponderà alla richiesta. L'informazione giungerà sia all'AP legale, che la scarterà a causa della client isolation, sia all'attaccante, che di nuovo si fingerà l'AP e trasmetterà l'informazione al Client 1. In questo modo la client isolation viene sconfitta.

L'implementazione di un anti client isolation è possibile tramite Airtun-ng della suite aircrack-ng. Esso permette di creare un'interfaccia virtuale nel sistema linux adatta sia al ricevimento di tutti i dati trasmessi da un certo BSSID, sia all'invio di pacchetti, siano essi inviati dallo stack normale TCP/IP, sia contraffatti (crafted) attraverso librerie netfilter. È stata concepita una proof of concept basata su scapy che agisce da relay di pacchetti appartenenti allo stesso dominio di broadcast. Il risultato è che la client isolation viene elusa fintanto che i client siano in range, oltre che dell'AP legale, del dispositivo che si occupa del relaying. A causa della bassa qualità dei componenti utilizzati per la PoC la velocità di trasferimento è molto ridotta, ma è possibile per esempio inviare pacchetti ICMP ping e ricevere la risposta tra Client 1 e Client 2 in presenza di Client Isolation. Poter eludere la client isolation ha come conseguenza la possibilità di eseguire ARP poisoning sulla rete, e quindi attacchi man in the middle (MITM).

3. Rogue Access Point

I Rogue Access Points sono l'altra minaccia per l'utente finale. Un RAP è un access point che annuncia un SSID noto (come ad esempio provinciawifi) ma è sotto il controllo di un attaccante. Si tenga presente che la gestione del Wi-Fi del sistema operativo del client esegue numerose operazioni in maniera trasparente per l'utente. Per esempio in mancanza di connessione si collega automaticamente ad un ESSID conosciuto, o si scollega da un AP e si collega ad un RAP se quest'ultimo offre un segnale molto migliore o se viene forzata una disconnessione dall'AP iniziale tramite un DeAuth attack. Una volta collegato ad un RAP l'utente finale è alla mercé dell'attaccante, poiché esso agisce da router ed è quindi in grado di intercettare le richieste e di mettere in atto attacchi di tipo MITM.

4. Attacchi MITM

Gli attacchi di tipo Man in the middle comporta-

no un certo grado di information disclosure. Gli attacchi prendono questo nome dal fatto che le comunicazioni tra client e server vengono intercettate da un attaccante che si pone in mezzo ed esegue operazioni di intercettazione (sniffing) o manipolazione di pacchetti. Affinché un attacco MITM possa essere effettuato l'attaccante deve in qualche modo poter frapporsi tra il client e il server in modo da poter controllare le connessioni. Questo vuol dire che precedentemente deve essere stato eseguito un ARP poisoning o il client bersaglio deve essere collegato ad un RAP sotto controllo dell'attaccante.

Un attacco di tipo MITM su una connessione in chiaro (http/smtp/pop/telnet) è completamente trasparente all'utente finale, mentre è rilevabile nel caso di connessioni SSL. Nelle connessioni SSL, infatti, è presente un certificato legato al nome a dominio che garantisce la sicurezza della connessione end-to-end. In caso di certificato contraffatto viene presentato un messaggio non facilmente ignorabile da parte dell'utente, se non altro nelle sessioni HTTPS.

5. SSLSTRIP

Più pericolosi per l'utente finale sono gli attacchi basati su sslstrip, un tool che in condizioni specifiche consente di evitare l'instaurarsi di connessioni HTTPS e di trasformarle in semplici HTTP, permettendo quindi di intercettare il traffico che passa in plain text. Per comprendere il funzionamento di sslstrip bisogna tenere presente come viene stabilita una connessione HTTPS.

In generale la connessione ad un server in HTTPS non avviene attraverso la scrittura diretta nella barra di indirizzi del browser, non si chiede quindi https://example.com

Quello che accade invece è che si giunga a https://example.com tramite:

a) Un link presente in una pagina di tipo http: <a href="https://example.com">

b) Un codice di reindirizzamento HTTP 302 che fa transitare da http://example.com a https://example.com

Se un attaccante ha predisposto un MITM attack può modificare i dati trasmessi, e trasformare l'href del caso a in un semplice <a href="http://example.com">. Lo stesso meccanismo permette di trasformare il codice di reindirizzamento e impedire che ci si sposti in HTTPS.

Un client che richiede una pagina web ad un server remoto mentre SSLSTRIP agisce da transparent proxy non troverà mai link HTTPS all'interno delle pagine, né accadrà mai che possa transitare in HTTPS tramite un codice 302. Al suo interno SSLSTRIP tiene una mappa delle richieste fatte dal client in maniera da poter eseguire le richieste HTTPS invece del client legittimo e di fornire le risposte corrette al client.

CLIENT <-----> http <-----> SSLSNIFF <-----> https <-----> LegitServer

Sslstrip, usato a seguito di altri attacchi rappresenta uno dei tool più insidiosi per catturare credenziali. Questo perché l'utente finale non è informato del fatto che la connessione su cui transitano le informazioni usa un certificato non valido, semplicemente transita tramite http.

6. HSTS

L'HTTP Strict Transport Security (HSTS) doveva essere la risposta ad attacchi di tipo sslstrip. HSTS permetteva di registrare nei browser informazioni riguardanti nomi a dominio che dovevano essere interrogati via HTTPS, e solo tramite esso, impedendo quindi che sslstrip potesse portare a termine l'attacco. Se l'utente richiede un sito per cui è presente un record HSTS il browser procede automaticamente ad un reindirizzamento interno (http code 307) e contatta il server remoto direttamente in HTTPS. I browser hanno una lista precompilata con i siti protetti da HSTS, ma è possibile per un server informare il client di aggiornare la lista HSTS con il proprio sito tramite un header particolare:

Strict-Transport-Security: max-age=expireTime [; includeSubdomains]

7. SSLSTRIP+

Al BlackHat Asia 2014 Leonardo Nve Egea ha presentato un fork di sslstrip che consente di inibire il funzionamento di HSTS in determinate condizioni. È impossibile impedire ad un browser di eseguire il reindirizzamento interno nel caso si scriva nella barra di indirizzi una url di cui è pre-

sente il record HSTS, ma è possibile modificare le pagine web http che contengono link protetti non solo strippando la parte sicura di HTTPS, ma anche modificandone il nome a dominio in qualcosa di simile (in maniera da non allarmare l'utente) ma comunque diverso dall'originale (impedendo quindi che venga riconosciuto dal browser come qualcosa per cui è presente un record HSTS). Per esempio nel tool di Nve il dominio google.com diventa gooogle.com.

8. Certificati Root Installati

Un'altra problematica per i client è quella che deriva dall'installazione nel proprio sistema operativo di un certificato root di proprietà dell'attaccante. Difficilmente gli utilizzatori finali sono a conoscenza di cosa sia questo tipo di certificato o di quali pericoli si corrano ad installarlo.

Se l'attaccante è in grado di eseguire un attacco MITM e riesce a convincere il client ad installare un proprio certificato root, sarà in grado di agire da transparent proxy direttamente via HTTPS, mostrando la famosa "chiave verde" all'interno dell'indirizzo, impedendo all'utilizzatore finale di capire di aver subito un attacco. SSLsniff esegue questo tipo di attacco.

9. Captive Portal

I Captive Portal sono un caso molto svantaggiato in questo contesto. Non possono essere protetti da HSTS in maniera preventiva, perché un attaccante può modificare il nome a dominio e sono, quindi, soggetti ad attacchi di tipo MITM, mettendo a repentaglio le credenziali di accesso. Combinando più attacchi si creano scenari complessi e in grado di ottenere le credenziali di accesso a reti anche ritenute più sicure, come ad esempio IDEM-Wifi, senza insospettire l'utente finale.

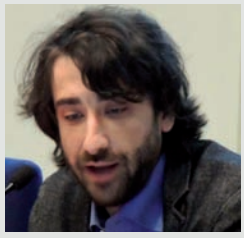
Sebbene l'utilizzo stock di sslstrip di primo acchito mostri l'inefficacia dell'attacco nei confronti dei sistemi di Single Sign On offerti da Shibboleth l'analisi delle risposte e le opportune modifiche ad sslstrip rendono possibile l'autenticazione dei client agli IdP basati su shibboleth e la cattura dei dati di autenticazione.

10. Conclusioni

Gli attacchi sopra descritti sono stati possibili perché prendevano di mira le due debolezze delle reti Wi-Fi aperte. Da una parte veniva sfruttato il fatto che la trasmissione dei dati avvenisse in chiaro: questo permetteva di utilizzare tecniche di anti isolation. Dall'altra si abusava del fatto che uno SSID da solo non garantisse l'identità dell'AP. 802.1x può essere la soluzione ai problemi di tipo client attack. Lo standard, già utilizzato ampiamente in ambito enterprise e colonna portante della rete eduroam, prevede l'utilizzo di chiavi private tra Access Point e Client che impedisce l'elusione della client isolation, e una forte crittografia in fase di autenticazione. Il baco classificato come Hole 196, per cui il traffico broadcast viene codificato con una chiave condivisa (GTK) tra i client potrebbe essere di qualche entità nel caso non fosse abilitata la client isolation. Ma in presenza di questa feature 802.1x si rivela our best bet per proteggere i client dagli attacchi di tipo MITM.

Riferimenti bibliografici

[1] http://www.thoughtcrime.org/software/sslstrip
[2] http://www.slideshare.net/Fatuo__/offensive-exploiting-dns-servers-changes-blackhat-asia-2014
[3] http://youtu.be/pAtup7n1BlI



Andrea Lora
andrea.lora@cnr.it

Lavora come system engineer presso il CNR all'Istituto di Cristallografia presso l'Area della ricerca di Montelibretti (RM1) in forza al Servizio Reti. Si occupa di virtualizzazione e storage, implementazione, amministrazione e monitoring di servizi e di network security. Attualmente è impegnato nell'implementazione di IPv6 nella rete dell'Area e nel miglioramento delle operazioni interne

Connettività a banda larga per le scuole torinesi Il Progetto Scuola 2.0

Marcello Maggiora[1], Calogero Martorana[2], Sandro Pera[3], Roberto Recchia[3]

[1]*Politecnico di Torino – Infrastructure IT Division*

[2]*CSI Piemonte – Direzione Architetture e Innovazione*

[3]*CSP – Innovazione nelle ICT - Direzione Innovazione*

Abstract. L'esigenza di intervenire sulle infrastrutture ICT scolastiche è oggi ampiamente sentita, la necessità di un ammodernamento dei servizi IT [1] ha assunto carattere di urgenza per rispondere agli impegni gestionali degli istituti e per supportare adeguatamente l'evoluzione dei modelli didattici. La sempre maggiore diffusione di nuovi setting di aula, genericamente indicati come "classi 2.0" [2] basati sull'accesso ai contenuti digitali disponibili su web, attraverso LIM, tablet e smartphone; l'adozione di modelli didattici di classe capovolta (flipped classroom); la recente tendenza ad introdurre processi formativi basati sul computational thinking [3], nonché la recente introduzione del cosiddetto "registro elettronico" rendono rilevanti due questioni: la prima è quella di un nuovo modello di insegnamento, basato su inquiry based learning e problem posing/solving per rendere gli studenti attivi e partecipi nel processo di costruzione delle loro conoscenze/competenze; la seconda è quella delle infrastrutture, intese come accesso alla rete, navigazione sicura, governo dei dispositivi e, più in generale, ottimizzazione delle risorse. La disponibilità di infrastrutture ICT adeguate è un fattore abilitante per lo sviluppo e l'evoluzione degli attuali modelli didattici. Questo lavoro presenta l'esperienza, maturata nell'arco degli ultimi 15 mesi, nel definire le linee progettuali, le analisi, le strategie di intervento fino alla fase esecutiva per fornire connettività a larga banda alle scuole primarie e secondarie di primo grado interessate dal progetto.

1. Il Progetto scuola 2.0

Il progetto nasce dalla volontà del MIUR, del Sindaco della Città di Torino e del Politecnico di Torino che, congiuntamente, hanno ritenuto di interesse strategico avviare un progetto pilota che affrontasse problematiche tecniche e organizzative per fornire un livello (medio) di informatizzazione degli istituti scolastici, non affidato ad iniziative estemporanee e non strutturate.

Il progetto vede coinvolti diversi enti del territorio, CSP-Innovazione nelle ICT (in breve CSP, Organismo di Ricerca accreditato presso il MIUR e soggetto tecnologico sperimentatore per Regione Piemonte rispetto all'innovazione in ambito ICT), CSI Piemonte (in breve CSI, ente attuatore dei servizi della PA sul territorio regionale Piemontese), Politecnico di Torino (in breve PoliTO) e Istituto Superiore Mario Boella (in breve ISMB, centro di ricerca applicata sulle ICT), che hanno collaborato fattivamente ad un progetto fortemente orientato a "fare sistema".

Coordinato dalla Città di Torino, è stato istituito un tavolo di lavoro dove sono stati definiti gli elementi progettuali, la ricerca delle risorse economiche a copertura dei costi del progetto e il modello di trasferimento alle scuole coinvolte, sia dei beni strumentali sia delle competenze necessarie alla corretta gestione degli impianti in corso di realizzazione. Per quanto riguarda i finanziamenti, significativo è stato il ruolo della Compagnia di San Paolo e del Comitato ICT, mentre i partecipanti hanno contribuito all'iniziativa non esponendo costi per le attività svolte.

Rilevante è stato lo sforzo del gruppo di lavoro di non concentrare l'attenzione su un solo aspetto, anche se fondamentale, come la connettività a banda larga, ma di impostare il lavoro per creare condizioni di fruibilità di tutti i componenti della catena di meta servizi, dal collegamento alla rete GARR fino a raggiungere l'attività di formazione in aula.

Ruoli, responsabilità e competenze sono oggetto di uno specifico Protocollo d'Intesa tra le parti coinvolte, mentre è in via di definizione un

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

Atto Convenzionale tra Città di Torino e Consortium GARR per la formalizzazione delle modalità di interconnessione delle scuole cittadine alla Rete della Ricerca.

2. Sviluppo del progetto

Dati gli obiettivi, il gruppo di progetto ha lavorato all'identificazione di un modello tecnico ed economico sostenibile per consentire alle scuole l'uso di risorse disponibili in rete per attività didattiche, attraverso la fornitura di collegamenti a banda larga.

Caratteristica abilitante è rappresentata dalla presenza del CSP nel gruppo di progetto che, nella sua qualità di ente accreditato dal consorzio GARR per operare a favore dell'integrazione delle scuole nel sistema di networking nazionale, svolge il ruolo di punto di raccolta di tutte le scuole afferenti. Assegnatario del piano di indirizzamento ha attivo un peering BGP con GARR attraverso il quale fornisce connettività Internet alle scuole.

Sono state messe a sistema le risorse tecniche ed infrastrutturali pubbliche già presenti in Piemonte (dal backbone regionale in fibra ottica realizzato dal CSI per conto della Regione Piemonte – programma WI-PIE – e dalla Provincia di Torino – Patti Territoriali – all'infrastruttura HPWNet – High Performance Wireless Network: ciò ha consentito di coinvolgere nel progetto un primo nucleo di 12 scuole. Quattro di queste in fibra ottica con il modello a IRU, con la realizzazione degli sbracci per il collegamento al backbone, e otto in radiofrequenza, con il collegamento alla dorsale wireless.

3. Interconnessione Wireless ed in Fibra Ottica

I collegamenti wireless alle scuole saranno realizzati in tecnologia Wi-Fi/Hiperlan, tramite l'impiego di apparati radio ed antenne conformi allo standard 802.11h/n in grado di operare alle frequenze di 2,4 GHz e 5 GHz. I collegamenti punto-punto saranno realizzati a partire dalla già citata dorsale di rete wireless HPWNet di CSP, che connette in banda ultra larga alcuni punti strategici dell'area metropolitana e della collina torinese, a loro volta collegati con decine di nodi distribuiti su tutto il territorio piemontese a distanze che variano dai 500 m agli 80 km. Per la realizzazione e gestione di HPWNet vengono utilizzati devices di diversi produttori e sistemi basati sull'asset Shelob di CSP, una piattaforma aperta che permette di customizzare e ottimizzare i driver del device, accrescendone le performance e consolidando l'affidabilità del sistema. La rete permette, quindi, anche il test di algoritmi e di protocolli innovativi di routing e forwarding e, prossimamente, per l'analisi in tempo reale della banda residua disponibile sulla tratta wireless.

L'interconnessione in fibra ottica seguirà una topologia a stella, il cui centro è localizzato nel nodo WI-PIE di Torino, sito presso la sede principale del CSI.

Fig. 1 Sito di dorsale HPWNet, cerchiato in rosso, visto dal tetto di una delle scuole coinvolte

Fig. 2 Porzione di Città di Torino in copertura radio da uno dei siti di dorsale HPWNet sulla collina torinese

Le attività di infrastrutturazione possono essere riassunte nei seguenti punti:

- posa di idonea canalizzazione per l'interconnessione dell'edificio scolastico con la dorsale esistente sul territorio;
- posa di fibra ottica nell'infrastruttura esistente dal punto di interconnessione fino al più vicino pozzetto di spillamento;
- giunzione delle porzioni di fibra ottica spenta presenti nelle dorsali già realizzate sul territorio fino ai cassetti ottici di centro stella;
- fornitura in diritto d'uso (IRU) per un periodo di 15 anni di una coppia di fibre spente per le tratte, in serie, tra gli edifici scolastici e il centro stella, comprensiva della manutenzione dell'infrastruttura per tutto il periodo del progetto.

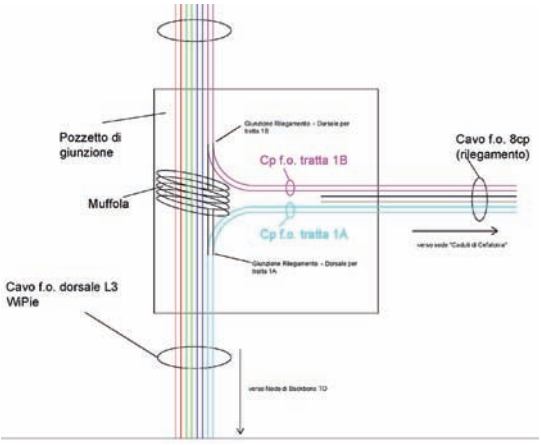


Fig. 3 Schema indicativo di giunzione "rilegamento-dorsale" nel punto di terminazione tratta

La fornitura è comprensiva di tutti gli elementi necessari alla consegna e al collaudo delle coppie di fibre ottiche spente fornite. Saranno forniti in opera tutti i componenti necessari alla realizzazione, manutenzione e gestione delle nuove tratte in fibra ottica spenta quali pozzetti di giunzione, muffole di giunzione, etc..

Le dorsali interessate appartengono al progetto regionale WI-PIE Linea3 e a quello provinciale Patti Territoriali. Esse si snodano lungo 6 direzioni diverse, genericamente rappresentate dalla figura 4.

4. Rete di raccolta

La rete di raccolta, dal punto di vista del networking, prevede un centro stella dual stack IPv4/IPv6 posto presso il CSP. Le tecniche di collegamento prevedono l'utilizzo di tecnologie differenti, a seconda che vi sia o meno la possibilità di trasportare una VLAN 802.1Q dal CSP fino all'apparato installato presso la scuola. Se non è possibile utilizzare il trasporto di livello 2, vengono utilizzate tecniche di trasporto alternative quali le VPN e classico routing con prestazioni elevate garantite dalla presenza di una sessione di peering su collegamento metroethernet tra il CSP e il Politecnico di Torino.

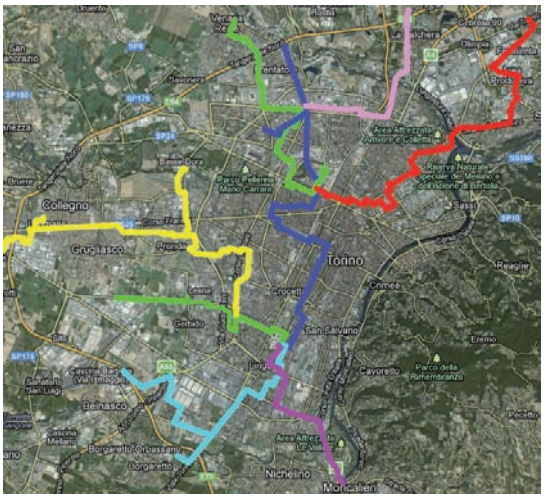


Fig. 4 Schema di generale delle dorsali sul territorio di Torino

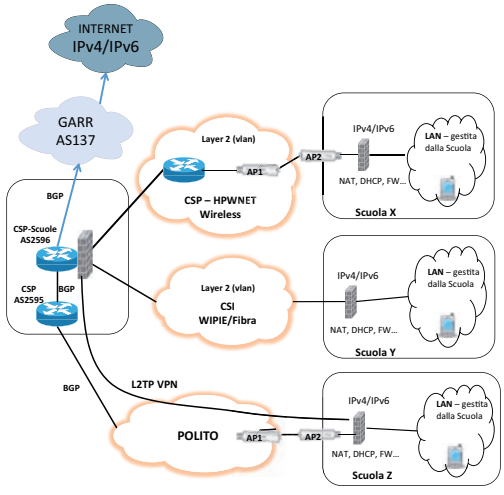


Fig. 5 Modello architetturale della rete, schema generale di interconnessione tra le scuole e la rete GARR

5. Infrastrutture interne

A livello delle singole LAN delle scuole, sono state condotte operazioni di ricognizione puntuale dell'esistente, in modo da definire il fabbisogno minimo per garantire la fruibilità del si-

stema di connettività da tutti i locali dell'edificio scolastico.

In molte delle scuole analizzate le dotazioni tecnologiche sono spesso risultate non adeguate agli standard attuali, limitate a vecchi apparati custoditi in laboratori non sempre collegati ad Internet. Il personale scolastico spesso non è stato in grado di dare risposte sulle modalità con cui la scuola era connessa e, a causa del turnover di dirigenti e tecnici, si sono stratificate soluzioni di connettività differenti. In alcuni casi le scuole risultano cablate per la telefonia (di competenza della Città), ma non per i dati.

MIUR ed Enti locali hanno progettato ed investito sulla connettività per garantire il funzionamento amministrativo della scuola; mentre gli aspetti legati alla didattica sono di competenza della singola scuola, che ha non poche difficoltà ad investire risorse in questa direzione. La carenza di competenze tecnologiche raramente permette alle scuole di negoziare condizioni eque con i fornitori di tecnologie e per questo, spesso, le stesse utilizzano consulenti esterni che fungono da tramite: in molti casi l'esiguità delle risorse impiegate porta ad accettare prestazioni di valore professionale non sempre adeguato. In generale questa frammentazione di interventi e competenze non genera efficienza e spesso penalizza la gestione da parte della scuole.

In ottica di riuso delle esperienze passate, si è preso spunto dall'esperienza positiva ottenuta con l'Associazione Dschola , che nel 2004 ha realizzato progetti innovativi riconosciuti anche a livello europeo. In particolare ha cercato di colmare il gap tecnologico esistente attraverso il supporto on-site e l'organizzazione di corsi di formazione nelle scuole. Questa esperienza, molto apprezzata, è stata messa a sistema nel progetto Scuola 2.0.

Al termine della fase di indagine, sono state individuate tre linee di intervento orientate a garantire un'infrastruttura funzionante ed affidabile:

1) *Connettività* – comporta interventi sulla connessione della scuola ad Internet, il cablaggio delle dorsali dell'istituto e la distribuzione interna in modalità wired/wireless;

2) *Dotazioni Tecnologiche* – ovvero rinnovamento degli elaboratori, attuabile attraverso il riuso di PC dismessi, oppure con soluzioni innovative, rendendo ad esempio utilizzabili anche dispositivi di proprietà degli studenti/docenti; o ancora utilizzando micro computer [4];

3) *Formazione per i referenti degli Istituti Scolastici* – la predisposizione di un piano formativo di aggiornamento sulle recenti tecnologie e soluzioni architetturali ICT, nonché di tecniche adeguate alla diagnosi dei malfunzionamenti dell'infrastruttura di rete in funzione delle soluzioni implementate. Competenze utili per interventi di primo livello e per interfacciare correttamente servizi di help desk e supporto tecnico.

Le scuole potranno usufruire di servizi di base con accesso ad Internet per i laboratori informatici e per gli apparati utilizzati per la didattica frontale (LIM, sistemi di videoconferenza, ecc.).

6. Sicurezza della rete

Per garantire la sicurezza di primo livello delle connessioni e un utilizzo non improprio della rete, sono state previste policy di sicurezza idonee all'ambito scolastico. In particolare, sarà tenuta traccia delle connessioni effettuate con l'uso di un sistema di logging; mentre la sicurezza sarà gestita in maniera centralizzata su un apparato con funzionalità di firewall, collocato nel centro stella della rete di connessione alle scuole afferenti al progetto, che raccoglierà il traffico di tutte le 12 scuole, interconnettendole al PoP GARR. Qui sarà applicata una soluzione di content filtering già positivamente adottata da altri istituti scolastici di vario ordine e grado, una soluzione Open-Source realizzata dall'Associazione Dschola. La soluzione implementata, trasparente e centralizzata, si trova nel centro stella posto presso il CSP (figura 6). Questa scelta offre diversi vantaggi: non è necessario configurare nulla lato scuola, si garantisce omogeneità nel trattamento del traffico ed è possibile mantenere aggiornato l'elenco dei contenuti bloccati (blacklist) in un unico punto.

Più nel dettaglio il traffico dati delle scuole passa attraverso un bridge trasparente dal quale viene estratto il traffico web (HTTP) tramite ebtables e rediretto sul proxy squid/squidguard

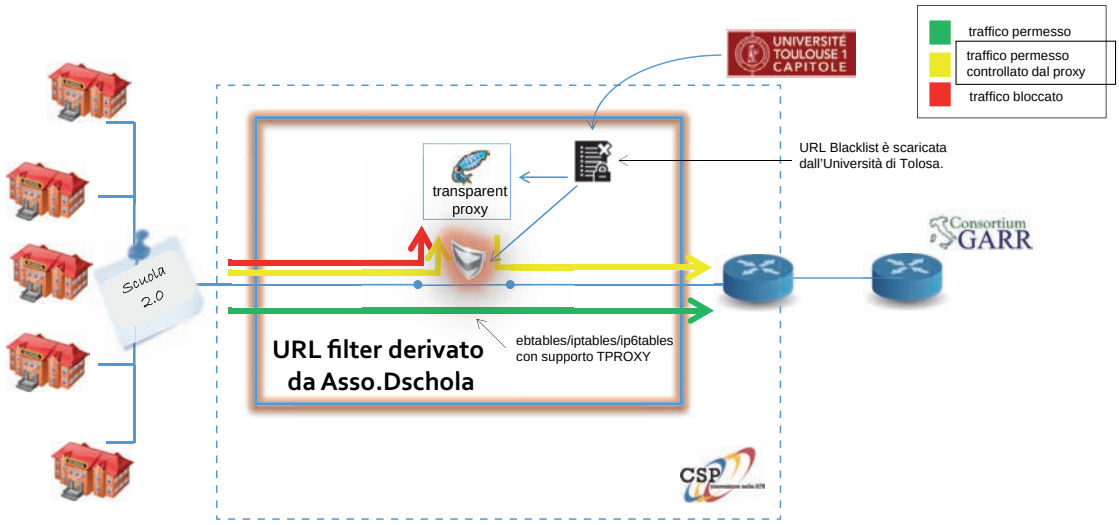


Fig. 6 Schema Content Filtering centralizzato

con iptables per essere analizzato. Sul bridge trasparente può passare un insieme di VLAN (IEEE 802.1q) dal quale si possono selezionare solo quelle di interesse. A livello IP sono supportati IPv4/IPv6 e il traffico che passa dal proxy web preserva le intestazioni IP (TPROXY) in modo che il sito di destinazione riceva i pacchetti con la sorgente IP originale del client e con cadenza giornaliera sono aggiornate le liste dall'Università di Tolosa.

7. Conclusioni

Lo sforzo richiesto per intervenire sulle infrastrutture ICT delle scuole, e quindi sugli strumenti di base per una didattica evoluta, è considerevole. Sono molte le componenti che devono essere prese in esame ed armonizzate opportunamente. Realizzare un piano di interconnessione completamente in fibra ottica del parco scolastico di una grande città può presentare costi e tempistiche difficilmente sostenibili. Il modello di interconnessione basato sulla coppia di soluzioni fibra ottica e link wireless offre l'opportunità di prevedere orizzonti temporali progettuali di breve/medio periodo, con costi gestibili e prestazioni adeguate.

Ciò non toglie che la fibra ottica rappresenti il mezzo cui tendere per soluzioni definitive. Tuttavia un'estesa rete in fibra ottica che raggiunga 180-200 edifici scolastici distribuiti sul territorio metropolitano presenta difficoltà di realizzazione non marginali; questa può invece essere realizzata più facilmente in background con una gestione integrata e coordinata delle attività di scavo e posa con impianti di tipo generale sull'area metropolitana. La rete in fibra ottica realizzata potrebbe per altro soddisfare altre esigenze di connettività che insistono sul territorio metropolitano, come per esempio i molti progetti legati alle Smart City. In questa direzione si è recentemente mossa la Città di Torino, stipulando un accordo con un operatore per la concessione in uso delle infrastrutture civili già esistenti per la posa di fibra ottica spenta, ed un primo blocco di opere di interconnessione con edifici di proprietà comunale ed edifici scolastici.

Ringraziamenti

Si desidera ringraziare i dirigenti scolastici e tutti i docenti/tecnici che hanno collaborato alla fase di analisi, la Città di Torino e gli assessorati competenti, in particolare l'assessorato all'Istruzione e Università, Politiche educative per l'infanzia e l'adolescenza direttamente coinvolto nelle varie fasi progettuali. Si ringraziano inoltre l'Istituto Superiore Mario Boella, ente strumentale della Compagnia San Paolo, ed il Comitato ICT per aver sostenuto finanziariamente il progetto. Infine, si desidera ringraziare il Prof. Marco Mezzalama per aver fornito il necessario impulso a tutto il progetto.

Riferimenti Bibliografici

[1] AA. VV., "Survey of Schools: ICT in Education", Final Study Report, European Commission, 2013

[2] C. E. Marchioro, S. Pera, P. P. Gruero, "La mobilità dei cittadini digitali, tra servizi smart della PA e della scuola del futuro", Quarto Convegno IDEM – GARR, 2014

[3] J. M. Wing, "Computational Thinking", Communication of the ACM, Vol.49 (3):33-35, 2006

[4] C. Edwards, "ICT lessons get the raspberry", IET Journals & Magazines, Engineering & Technology, Vol.7 (4):76-78, 2012

Marcello Maggiora
marcello.maggiora@polito.it

Ingegnere Informatico, è responsabile delle Infrastrutture IT del Politecnico di Torino, nel suo percorso professionale si è occupato di diverse aree tecnico scientifiche: computer grafica, database multimediali, tecnologie web, piattaforme di calcolo, reti di calcolatori e wsn. È ricercatore associato presso il Computer Engineering and Networks Group del CNR.

Calogero Martorana
calogero.martorana@csi.it

Laureato in Lettere, da 30 anni nell'ICT, prima come responsabile dei Sistemi Informativi dello IACP di Torino e dal 1999 in CSI Piemonte, lavorando su importanti progetti infrastrutturali (scuole, EE.LL., connettività satellitare rifugi alpini). Oggi segue i progetti di wi-fi pubblico della Città di Torino e i servizi ICT di alcune agenzie regionali.

Sandro Pera
sandro.pera@csp.it

Lauratosi in Ingegneria delle Telecomunicazioni al Politecnico di Torino, da oltre dodici anni si occupa di reti wireless a banda larga e più recentemente a banda stretta per l'IoT, e di progetti sperimentali sul territorio. Oggi ricopre il ruolo di Wireless Networks Programme Developer in CSP.

Roberto Recchia
roberto.recchia@csp.it

Laureatosi in Ingegneria Elettronica con indirizzo in Telecomunicazioni al Politecnico di Torino, da oltre quindici anni si occupa di progettazione, realizzazione e gestione in ambito networking. Oggi ricopre il ruolo di Network and System Manager & ICT Project Engineer in CSP.

Time-Frequency Packing per sistemi ottici ad alta capacità

Marco Secondini[1], Tommaso Foggi[2], Francesco Fresi[1], Gianluca Meloni[2], Antonia Mastropaolo[1], Fabio Cavaliere[3], Giulio Colavolpe[4], Enrico Forestieri[1], Luca Potì[2], Roberto Sabella[3], Giancarlo Prati[2]

[1]Scuola Superiore Sant'Anna, [2]CNIT, [3]Ericsson Research Italia, [4]Università degli Studi di Parma

Abstract. In questo lavoro viene presentata l'applicazione del Time-frequency Packing (TFP), uno schema di modulazione attraverso il quale è possibile ottenere la massima efficienza spettrale utilizzando formati di modulazione e detector a complessità limitata. Il lavoro analizza i principi teorici sui quali la tecnica si basa, illustra le procedure di design e l'implementazione del sistema ponendo l'attenzione sugli aspetti peculiari dell'applicazione del TFP. In particolare, la compensazione adattiva degli effetti dovuti alla propagazione in fibra ottica, il filtraggio adattato, la rivelazione basata sulla probabilità Maximum a Posteriori sono ottenuti dalla combinazione di un equalizzatore di tipo feed-forward e da quattro detector BCJR. Sono stati, inoltre, progettati dei codici LDPC irregolari con differenti rate per ottenere la massima efficienza spettrale per differenti rapporti segnale-rumore. Viene, infine, fornita la dimostrazione sperimentale del design del sistema.

1. Introduzione

I sistemi di comunicazione ottica di nuova generazione impiegano la rivelazione coerente in combinazione con tecniche di Digital Signal Processing avanzato per ottenere alti "rate" trasmissivi. Le attuali implementazioni caratterizzate da capacità di 100 Gb/s consentono il raggiungimento di valori di efficienza spettrale intorno ai 2 bit/s/Hz. Pur considerando le limitazioni di potenza e banda dei link in fibra, esistono ancora notevoli margini di miglioramento in termini di capacità del canale rispetto alle tecnologie attualmente sviluppate.

Allo scopo di incrementare l'efficienza spettrale rispetto ai sistemi attualmente realizzati è necessario adottare uno schema di modulazione in grado di fornire le migliori prestazioni in termini di energia, costi e affidabilità per un dato SNR e per determinati vincoli di complessità.

Nelle comunicazioni ottiche viene tipicamente utilizzata la segnalazione ortogonale come nel caso del Nyquist WDM e del OFDM [1]-[3]. Il rispetto della condizione di ortogonalità imposto in questo tipo di segnalazione vincola la scelta della spaziatura nel dominio del tempo e della frequenza, assicurando una trasmissione priva di interferenza intersimbolica (ISI) e interferenza tra portanti (ICI) alle spese di un valore della massima efficienza spettrale del sistema limitato in relazione al numero di livelli del formato di modulazione utilizzato. Infatti, per ottenere alti valori di efficienza spettrale è necessario l'impiego di formati di modulazione multilivello con alta complessità e bassa sensibilità agli effetti non lineari.

Alcuni degli approcci proposti recentemente, superando il limite di Nyquist, consentono di ottenere maggiore efficienza spettrale pur utilizzando formati di modulazione poco complessi [4]-[8].

Il Time Frequency Packing (TFP) rappresenta un'evoluzione del già noto Faster-than-Nyquist (FTN) [9] e può essere considerato come una procedura di design per l'ottimizzazione di una classe di formati di modulazione.

L'approccio utilizzato nel time-frequency packing è quello di suddividere il problema in tre parti fissando dapprima la costellazione che si intende utilizzare e la complessità del detector, trovando l'ottimo time-spacing and fre-

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5

quency-spacing che fornisce la massima efficienza spettrale ottenibile con quella data costellazione e complessità del detector e selezionando, infine, un codice da applicare per ottenere la suddetta efficienza spettrale.

2. Time-frequency packing

Per analizzare gli aspetti teorici che stanno alla base del TFP facciamo riferimento all'equivalente passa-basso di un sistema che utilizza un tale approccio (Fig. 1).

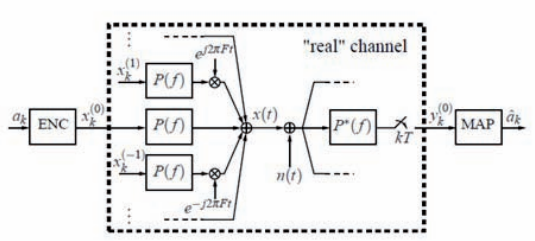


Fig. 1 Sito di dorsale HPWNet, cerchiato in rosso, visto dal tetto di una delle scuole coinvolte

Le portanti sono equispaziate e vengono modulate tutte con lo stesso formato di modulazione e con lo stesso impulso formante *p(t)*. L'inviluppo complesso del segnale è:

$$x(t) = \sum_l \sum_k x_k^{(l)} p(t - KT)\, e^{j2\pi lFt} \quad (1)$$

dove sono indicati rispettivamente con $x_k^{(l)}$ il simbolo trasmesso sulla *l*-esima portante al tempo *kT*, con *T* la spaziatura temporale tra i simboli e con *F* la spaziatura frequenziale tra portanti adiacenti. Assumendo di poter considerare il link ottico come un canale ideale a doppia polarizzazione affetto da rumore additivo Gaussiano bianco (AWGN) *n(t)*, il segnale corrotto dal rumore sarà demodulato attraverso l'uso di filtri adattati e di campionatori a tempo di simbolo. L'efficienza spettrale di tale sistema risulta essere:

$$\eta = \frac{I(X;Y)}{FT} \quad (2)$$

dove I(X;Y) rappresenta il termine di informazione mutua tra input e output e FT è il prodotto tempo-frequenza.

Allo scopo di evitare l'insorgere di fenomeni di ISI e ICI sarebbe necessario progettare lo schema di modulazione nel rispetto della condizione di ortogonalità e ponendo quindi dei vincoli sull'impulso formante e sulla spaziatura frequenziale e temporale tra gli impulsi (limite di Nyquist). Utilizzando la segnalazione ortogonale, I(X;Y) si ottiene impiegando un symbol-by-symbol detector e dipende solamente dal formato di modulazione e dal rapporto segnale rumore. Il rispetto del limite di Nyquist impone però che il prodotto FT sia unitario e dunque, l'unico modo per incrementare in questo caso l'efficienza spettrale è quello di aumentare la cardinalità del formato di modulazione utilizzato.

Se si sceglie invece di non utilizzare la segnalazione ortogonale decadono i vincoli su p(t), F e T ed è quindi possibile scegliere p(t) in base ai componenti hardware disponibili e ridurre il prodotto FT oltre il limite di Nyquist senza modificare il formato di modulazione. L'utilizzo di una segnalazione di tipo non ortogonale introduce però fenomeni di interferenze nel sistema (ICI e ISI) che agiscono riducendo il numeratore della (2) e rendono necessario l'impiego di un detector più complesso. L'obiettivo in questo caso è quindi quello di selezionare F e T in modo che la riduzione del numeratore sia più che bilanciata dalla riduzione del denominatore e che il detector non abbia complessità troppo elevata. Il Faster-than-Nyquist (FTN) opera assicurando che la spaziatura temporale e quella frequenziale vengano selezionate mantenendo la minima distanza euclidea del sistema (Mazo limit e two-dimensional Mazo limit).

L'approccio del TFP è invece quello di fornire l'ottimo in termini di efficienza spettrale dato l'utilizzo di un detector di una data complessità. A questo scopo viene utilizzata una definizione leggermente diversa per l'efficienza spettrale, ottenuta sostituendo il termine di muta informazione I(X;Y) con l'information rate massimo ottenibile per un decoder non adattato (achievable information rate-AIR) [10].

Lo AIR è definito come segue:

$$\hat{I}\left(X^{(0)};\, Y^{(0)}\right) \triangleq \lim_{k\to\infty} \frac{1}{K} E\left\{\log \frac{q\left(x^{(0)}|y^{(0)}\right)}{q\left(y^{(0)}\right)}\right\} \le I(X;Y) \quad (3)$$

dove $x^{(0)}$ e $y^{(0)}$ sono i k simboli rispettivamente trasmessi e ricevuti sul canale 0 e $q\,(x^{(0)} \mid y^{(0)})$ e $q\,(y^{(0)})$ sono le distribuzioni di uscita condizionale e marginale ottenute connettendo l'input a un canale ausiliario arbitrario. La quantità espressa in (3) rappresenta un limite inferiore per l'informazione mutua, inoltre, si può ottenere attraverso il MAP (Maximum a Posteriori) un detector progettato per il canale ausiliario selezionato e può essere valutata in maniera semplice attraverso le simulazioni. Il canale ausiliario viene selezionato come quello che fornisce il miglior compromesso tra prestazioni e complessità, tanto più esso risulta essere simile al canale reale tanto più $\hat{I}$ è simile a I. Più semplice è il canale ausiliario, più semplice è il MAP detector per ottenere $\hat{I}$. Infine, le spaziature nel tempo e nella frequenza sono ottimizzate massimizzando l'efficienza spettrale ottenibile con il detector selezionato.
L'efficienza spettrale che si ottiene con l'applicazione del TFP è la seguente:

$$\hat{\eta} = \max_{F,T>0} \frac{\hat{I}(X^{(0)}; Y^{(0)})}{FT} \leq \eta \qquad (4)$$

L'approccio innovativo del TFP rispetto al FTN consiste nel trovare l'ottimo del prodotto BT e del rapporto F/T utilizzando l'espressione (4), selezionare uno dei parametri (F,T o B) in maniera arbitraria e calcolare gli altri di conseguenza. L'efficienza spettrale aumenterà con il crescere del rapporto segnale rumore, ma i valori ottimi di F e T dipendono solo in minima parte da SNR, tanto che una singola ottimizzazione può essere adottata per un ampio range di SNR.
L'ultimo step del TFP, comune a quasi tutti i sistemi di comunicazione digitale, consiste nel trovare una strategia di codifica tale che, codificando in maniera appropriata i bit di informazione sui simboli trasmessi $\{x_k^{(0)}\}$, si è in grado di ottenere un valore di efficienza spettrale il più vicino possibile a (4).

3. Design del sistema

Per il design di un sistema ottico multiportante che utilizza il TFP è stata utilizzata la modulazione DP-QPSK a un rate 1/T con impulsi formanti p(t). Tutte le portanti modulate vengono combinate e trasmesse su un canale AWGN con rumore n(t). Al ricevitore la portante viene demodulata tramite un filtro adattato e un campionatore a tempo di simbolo. I campioni ricevuti vengono inviati a un MAP symbol detector basato sull'algoritmo BCJR. Il detector è adattato al canale ausiliario il quale rappresenta un'approssimazione del canale reale ottenuta trascurando l'ICI, troncando l'ISI ai primi L_T simboli ed incrementando la varianza del rumore in modo da tener conto dell'ICI trascurato e dell'ISI.
Sebbene l'impulso formante può essere ottimizzato per incrementare l'efficienza spettrale, consideriamo in questo lavoro soltanto impulsi ottenuti impiegando filtri di Chebyshev del nono ordine con banda a -3 dB pari a B. Dato l'impulso p(t), attraverso l'uso di simulazioni numeriche, vengono ottimizzate l'efficienza spettrale e le spaziature temporale e frequenziale. Tale ottimizzazione viene eseguita considerando una memoria di canale di lunghezza pari a L_T =3 per due valori del rapporto segnale rumore rispettivamente pari a 7.5 e 22.5 dB. La massima efficienza spettrale si raggiunge codificando il segnale con codici LDPC progettati ad-hoc per un canale affetto da ISI. La procedura adottata per la costruzione di tali codici si esplica in due step. Viene dapprima utilizzata la tecnica euristica proposta in [11] per l'ottimizzazione del grado di distribuzione dei variable e dei check node e successivamente viene costruita la matrice di parità con tale grado di distribuzione attraverso algoritmi PEG (Progressive Edge Growth).

4. Implementazione del sistema

Un sistema in fibra ottica basato sul TFP utilizza la stessa configurazione hardware di un tipico sitema WDM basato sulla rivelazione coerente [12]. La figura 2 presenta lo schema descrittivo del sistema al quale facciamo riferimento. Tale sistema è di tipo single user detector in quanto presenta un trasmettitore e un ricevitore indipendente per ciascuna portante ottica. Ogni singola portante generata attraverso un laser di tipo ECL (external-cavity laser) alla lunghezza d'onda desiderata viene modulata per poi essere combinata attraverso un multiplexer ottico con

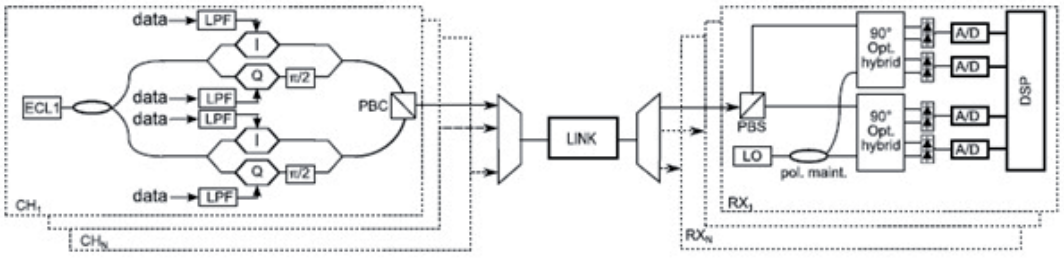


Fig. 2 Schema del trasmettitore e ricevitore di un sistema basato sul Time-frequency Packing

le altre portanti. Una volta trasmessa sul canale ottico, ciascuna portante viene estratta attraverso un demultiplexer ottico e rivelata in modo indipendente.

In ciascun trasmettitore lo schema di modulazione adottato per ogni componente in fase e in quadratura dei due stati di polarizzazione è basato sull'uso di un modulatore Mach-Zender pilotato a basso voltaggio e di un filtro elettrico. La scelta di un tale schema è dovuta al fatto che esso rappresenta la migliore scelta in termini di costi e complessità.

Al ricevitore viene utilizzato un tipico schema basato su rivelazione coerente. Dopo il demultiplexing ogni portante viene divisa nei due stati di polarizzazione ortogonali ciascuno dei quali viene combinato separatamente con il campo ottico di un oscillatore locale all'interno di un ibrido ottico 90°, e rivelato con due coppie di fotodiodi bilanciati. Il campionamento dei segnali all'uscita dai fotodiodi viene effettuato attraverso un convertitore analogico-digitale (ADC) con banda B pari almeno alla banda dell'inpulso p(t) e frequenza di campionamento pari a 2B. L'altra parte dei ricevitore è costituita da un sistema di processing digitale illustrato nello schema in figura 3, supponendo di avere frequenza di campionamento 1/T. Dato che si utilizza il TFP, la banda e la frequenza di campionamento richieste sono tipicamente inferiori a 1/(2T) e 1/T rispettivamente, pertanto viene effettuato un sovracampionamento per ottenere la frequenza 1/T richiesta per il processing. Ciascun campione complesso ricevuto r_k viene processato per compensare l'offset di frequenza tra il segnale e l'oscillatore locale. La stima di tale offset è effettuata sulla base di sequenze di training utilizzando l'algoritmo [13]. I campioni compensati s_k vengono dati in ingresso a un 2D-FFE (two dimensional feed-forward equalizer) attraverso il quale vengono compensati gli effetti lineari della propagazione quali group-velocity dispersion (GVD), rotazione di polarizzazione e polarization-mode dispersion (PMD). I campioni equalizzati delle due polarizzazioni $z_{1,k}$ e $z_{2,k}$ vengono elaborati separatamente per compensare il rumore di fase del laser (carrier phase estimation CPE) la cui stima si basa sull'algoritmo di Tikhonov. Infine, ciascuna componente in fase e in quadratura viene inviata separatamente a un detector BCJR con 2^{LT} stati seguito dal decoder LDPC. Lo schema di rivelazione utilizzato è di tipo MAP basato sul modello di Ungerboeck [14]-[15], e viene ottenuto attraverso uno scambio iterativo di informazioni tra i detector BCJR [16] e i decoder LDPC[17].

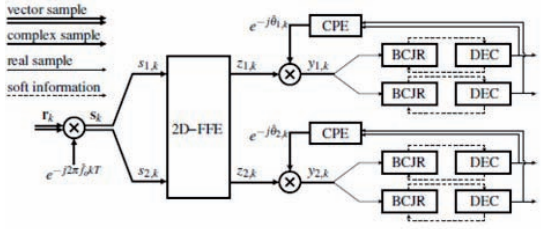


Fig. 3 Schema del DSP

5. Dimostrazione Sperimentale

Il setup sperimentale utilizzato per l'implementazione di un sistema basato su TFP è illustrato in figura 4.

I cinque laser ECL vengono modulati separatamente per mezzo di due modulatori Mach-Zehnder annidati.

La spaziatura frequenziale, ottimizzata secondo la procedura descritta precedentemente, è impostata a F=20 GHz e i segnali che pilota-

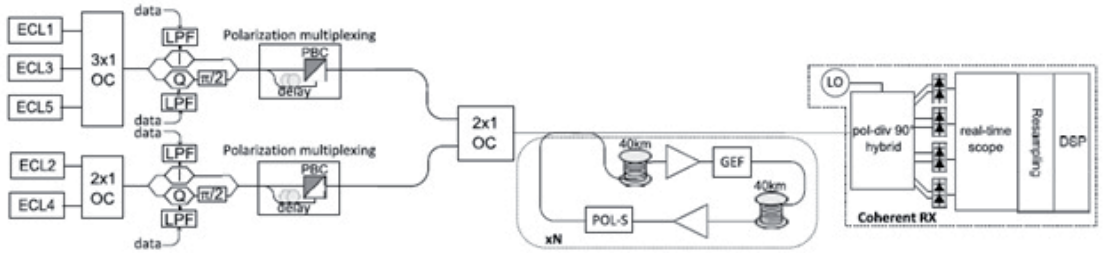


Fig. 4 Setup sperimentale

no la componente in fase e in quadratura di ciascun IQ-MZM sono modulati a frequenza R=1/T = 40 GBd e filtrati con filtri di Chebyshev del nono ordine con banda B=10 GHz. La tensione picco-picco di modulazione V_{PP} è pari a 1.5 V mentre la tensione V_{π} è pari a 2.8. Il multiplexing delle polarizzazioni è emulato per mezzo di un beam splitter 50/50, una linea di ritardo ottica e un polarization beam combiner (PCB). Le componenti I e Q modulate da bit di informazione random vengono codificate attraverso un codice LDPC opportunamente progettato. I canali pari e dispari sono accoppiati utilizzando un accoppiatore ottico 2x1.

Uno dei cinque canali viene rivelato dopo la trasmissione utilizzando uno schema di rivelazione coerente a diversità di fase e di polarizzazione che impiega un oscillatore locale (LO) che trasmette alla stessa lunghezza d'onda nominale del segnale ricevuto. I segnali rivelati da quattro coppie di fotodiodi bilanciati vengono campionati a 50 GSa/s attraverso un oscilloscopio real time con banda 20 GHz. Dopo un ricampionamento digitale alla frequenza 1/T il segnale ricevuto viene elaborato off-line secondo lo schema di processing visto nella sezione precedente.

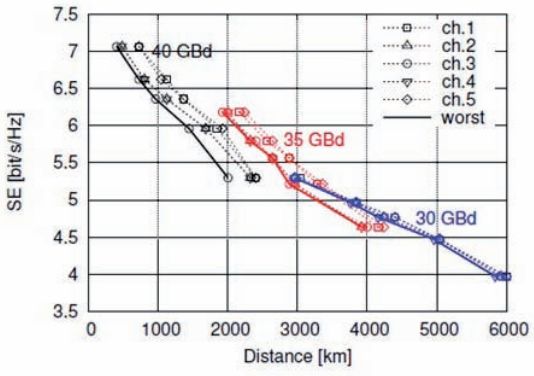


Fig. 5 Risultati sperimentali ottenuti con le configurazione a 40 GBd, 35 GBd e 30 GBd

I risultati sperimentali ottenuti utilizzando il setup appena descritto dimostrano che su distanze di 6000 Km, riprodotte sperimentalmente attraverso un recirculating loop, il sistema presenta efficienza spettrale pari a 4 bit/s/Hz. Su una distanza di 300 Km si è ottenuto il valore record di 7.1 bit/s/Hz.

Riferimenti bibliografici

[1] G. Bosco, V. Curri, A. Carena, P. Poggiolini, and F. Forghieri, "On the performance of Nyquist-WDM Terabit superchannels based on PMBPSK, PM-QPSK, PM-8QAM or PM-16QAM subcarriers," J.Lightwave Technol., vol. 29, no. 1, pp. 53–61, 2011.

[2] W. Shieh, X. Yi, and Q. Yang, "Coherent optical OFDM: has its time come?," vol. 7, pp. 234–255, Mar.2008.

[3] A. Barbieri, G. Colavolpe, T. Foggi, E. Forestieri, and G. Prati, "OFDM vs. single-carrier transmission for 100 Gbps optical communication,"J. Lightwave Tech., vol. 28, pp. 2537–2551, September 1 2010.

[4] A. Barbieri, D. Fertonani, and G. Colavolpe, "Time-frequency packing for linear modulations: spectral efficiency and practical detection schemes," IEEE Trans. Commun., vol. 57, pp. 2951–2959, Oct. 2009.

[5] G. Colavolpe, T. Foggi, A. Modenini, and A. Piemontese, "Faster-than-Nyquist and beyond: how to improve spectral efficiency by accepting interference," Opt. Express, vol. 19, pp. 26600–26609, December 2011.

[6] L. Potí, G. Meloni, G. Berrettini, F. Fresi, M. Secondini, T. Foggi, G. Colavolpe, E. Forestieri, A. D'Errico, F. Cavaliere, R. Sabella, and G. Prati, "Casting 1 Tb/s DP-QPSK communi-

cation into 200 GHz bandwidth," in Proc. European Conf. on Optical Commun. (ECOC'12), September 19-23, 2012.

[7] N. Sambo, G. Meloni, F. Paolucci, F. Cugini, M. Secondini, F. Fresi, L. Poti, and P. Castoldi,"Programmable transponder, code and differentiated filter configuration in elastic optical networks," J. Lightwave Tech., vol. 32, pp. 2079–2086, June 2014.

[8] G. Colavolpe and T. Foggi, "Time-frequency packing for high capacitycoherent optical links," IEEE Trans. Commun., vol. 62, pp. 2986–2995,Aug 2014.

[9] J. E. Mazo, "Faster-than-Nyquist signaling," Bell System Tech. J., vol. 54,pp. 1450–1462, Oct. 1975.

[10] N. Merhav, G. Kaplan, A. Lapidoth, and S. S. Shitz, "On information rates for mismatched decoders," IEEE Trans. Inform. Theory, vol. 40, pp. 1953–1967, Nov. 1994.

[11] S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," IEEE Trans. Commun.,vol. 52, pp. 670–678, Apr. 2004.

[12] G. Colavolpe, T. Foggi, E. Forestieri, and G. Prati, "Robust multilevel coherent optical systems with linear processing at the receiver," J. Lightwave Technol., vol. 27, pp. 2357–2369, July 2009.

[13] U. Mengali and M. Morelli, "Data-aided frequency estimation for burst digital transmission," IEEE Trans. Commun., vol. 45, pp. 23–25, January 1997.

[14] G. Ungerboeck,"Adaptive maximum-likelihood receiver for carriermodulated data-transmission systems," IEEE Trans. Commun., vol. 22, pp. 624–636, May 1974.

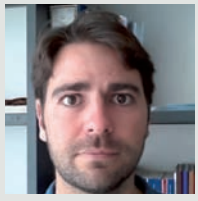
[15] G. Colavolpe and A. Barbieri,"On MAP symbol detection for ISI channels using the Ungerboeck observation model," IEEE Commun. Letters, pp. 720–722, August 2005.

[16] R. Bahl, J. Cocke, F. Jelinek, and R. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," IEEE Trans. Inform. Theory, vol. 20, pp. 284–284, Mar. 1974.

[17] S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," IEEE Trans. Commun.,vol. 52, pp. 670–678, Apr. 2004.

Marco Secondini
marco.secondini@sssup.it

Marco Secondini ha conseguito il dottorato di ricerca presso la Scuola Superiore Sant'Anna di Pisa nel 2006, dove è attualmente ricercatore. Si occupa di sistemi di comunicazione in fibra ottica ed è coordinatore nazionale del progetto FIRB "Coherent Terabit Optical Networks".


Tommaso Foggi


Francesco Fresi


Gianluca Meloni


Antonia Mastropaolo

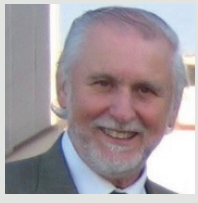

Fabio Cavaliere


Giulio Colavolpe


Enrico Forestieri


Luca Potì


Roberto Sabella


Giancarlo Prati

La localizzazione indoor nel mondo dell'IoT

Lorenzo Palma

Università Politecnica delle Marche

Abstract. Il mondo degli Smart-Objects è un mondo completamente nuovo e se migliaia di produttori vanno in migliaia di direzioni diverse ne consegue che ognuno svilupperà il suo prodotto ma non garantirà la nascita di un unico sistema interconnesso ed interoperabile. Internet of Things (IoT) rappresenta un universo in continua espansione e se si vuole garantire l'evoluzione, la scalabilità, l'utilizzo in diversi contesti applicativi, la compatibilità con diverse tecnologie di comunicazione e, soprattutto, l'interoperabilità diventa necessario seguire delle regole comuni. Proprio dal soddisfacimento di queste necessità e dalla stretta collaborazione fra Università ed Industria nasce WiSeNet che rappresenta il giusto compromesso fra conoscenza, esigenze del mercato, alta qualità del prodotto ed innovazione.

1. WiSeNet

WiSeNet nasce seguendo la filosofia del sistema operativo Contiki che rappresenta l'elemento centrale dello stack per IoT sviluppato. Contiki fornisce dei meccanismi utili a chi sviluppa Smart-Objects Network come quelli per le comunicazioni dei nodi con il mondo circostante, quelli per limitare il consumo di potenza da parte del dispositivo radio ed, inoltre, fornisce librerie per la gestione della memoria e delle liste dinamiche. Ha un file system che permette ai programmi di utilizzare le memorie flash come dei tradizionali hard-disk. Contiki è stato il primo sistema operativo per Smart-Objects a consentire la comunicazione IP fra i nodi della rete attraverso il protocollo µIP. L'intero stack protocollare sviluppato all'interno del gruppo di ricerca che segue la filosofia dettata dell'architettura Contiki, è basato su indirizzamento IPv6 ed appositamente progettato per avere basso foot print, questo lo rende perfettamente adatto a lavorare con la piattaforma hardware sviluppata sulla base degli stringenti requisiti dettati dal mondo industriale relativamente al basso costo ed al basso consumo energetico.

Il nodo sensore realizzato si basa su componentistica low cost come quella prodotta da STMicroelectronics ed è equipaggiato con il transceiver Spirit1 configurato per operare nella banda degli 868MHz ed un microcontrollore della famiglia STM32L1 noti per le caratteristiche Ultra Low Power. Sfruttando l'interoperabilità e la modularità dello stack si potrebbe sostituire la radio, ad esempio con una a 2.4GHz, lavorando soltanto sui driver di basso livello e lasciando inalterati i protocolli dal livello Data Link in su. La stessa operazione potrebbe essere eseguita per qualsiasi altro hardware voglia essere utilizzato per la creazione di un dispositivo per l'IoT che sfrutti l'architettura realizzata.

I primi due livelli dello stack implementano 802.15.4, in particolare a livello fisico si è scelto di lavorare nelle frequenze Sub GHz utilizzando una radio che può essere configurata per operare dai 169MHz ai 915MHz semplicemente cambiando il valore della componentistica passiva di configurazione; in questa trattazione si è scelto di operare a 868MHz. Salendo al livello Data Link si è implementata la tecnica del CSMA-CA. Un livello intermedio tra il primo ed il secondo prende il nome di Radio Duty Cycling (RDC) ed è responsabile dell'ottimizzazione dei consumi energetici della radio che sono ridotti al minimo attraverso una gestione attentamente progettata dei tempi di Sleep, di TX e di RX, nonché dei messaggi scambiati all'interno della rete mesh relativamente alla negoziazione delle migliori rotte per l'instradamento dei messaggi.

Salendo di livello troviamo un layer adattativo necessario affinché i flussi provenienti dai livelli superiori con una MTU pari a 1280 Bytes

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

possano essere incapsulati all'interno di frame 802.15.4 tipicamente di 127 Bytes. Questo lavoro viene svolto da 6LowPAN che ha, fra gli altri, il compito di gestire frammentazione e compressione degli header dei pacchetti in discesa.
A livello superiore troviamo µIP ovvero un'implementazione del tradizionale protocollo IP realizzata appositamente per gli Smart-Objects o per dispositivi embedded. µIP implementa i tradizionali protocolli della suite IP di livello rete e trasporto come IP, ICMP, UDP e TCP. µIP è il primo stack per dispositivi embedded che implementa anche il protocollo TCP. Vediamo come lavora:

- Appena un pacchetto viene ricevuto dal dispositivo di comunicazione viene chiamata la funzionalità "input process" che si occupa di analizzare l'header del pacchetto IP. Tale funzione verifica il contenuto del pacchetto e lo inoltra ai livelli superiori.
- La funzionalità di "output process" viene richiamata da µIP quando l'applicazione ha prodotto dati da inviare. È µIP che stabilisce quando dei dati in uscita possono essere passati al dispositivo di comunicazione. Prima di passare questi dati la funzione di output aggiunge gli opportuni header al pacchetto.
- µIP ha una funzionalità che viene ripetuta periodicamente (periodic process) che ha lo scopo di verificare se qualche applicazione deve ritrasmettere dei dati o se qualche connessione deve essere chiusa.
- Inoltro e routing dei pacchetti sono gestiti a parte.

Come protocollo di routing è stato utilizzato il Routing Protocol for Low Power and Lossy Network (RPL). RPL costruisce un DODAG (Destination Oriented Directed Acyclic Graph), ogni percorso nel grafo è costruito da un nodo della rete verso il nodo root. Nel DODAG di RPL ogni nodo presenta percorsi alternativi verso gli altri nodi della rete e verso il root. Questa scelta è utile ad ovviare al problema di inaffidabilità dei collegamenti wireless a bassa potenza. RPL definisce tre nuove tipologie di messaggi di controllo ICMPv6 che vengono utilizzati per la costruzione del grafo. I nuovi messaggi definiti da RPL sono il DIO (DODAG Information Object), il DAO (DODAG Advertisement Object) ed il DIS (DODAG Solicitation Object). La rete è una mesh autoconfigurante ed autoinstallante e questo significa che è sufficiente accendere i vari nodi affinché questi siano visibili e direttamente configurabili ed interrogabili dal web. L'indirizzamento avviene tramite l'assegnazione di un indirizzo IPv6 per ciascun nodo che a tutti gli effetti diventa univocamente identificabile e raggiungibile dalla rete internet globale dando vita al concetto di IoT.

Come protocolli di trasporto sono implementati UDP e TCP. All'interno di ciascun nodo di WiSeNet può essere implementato un client http o CoAP per la gestione delle richieste provenienti dal Web e la raccolta dati dai sensori secondo il paradigma REST.

2. Localizzazione Indoor

Fra le molteplici applicazioni sviluppate nel mondo dell'IoT (monitoraggio ambientale, applicazioni per l'AAL, sensoristica indossabile e contact-less, servizi di logistica, agricoltura intelligente) si è scelto di analizzare e sfruttare le caratteristiche della rete per un'applicazione che suscita molto interesse nel mondo industriale per le potenziali applicazioni sia nel pubblico che nel privato ovvero la localizzazione indoor.
La tecnica sviluppata si avvantaggia delle caratteristiche del canale radio a 868MHz e come tutte le tecniche già note in letteratura consta di due fasi: Ranging e Positioning. Il primo avviene tramite RSSI, mentre per il secondo si è implementato l'algoritmo del MIN-MAX con alcune varianti appositamente studiate per l'adattabilità a dispositivi Ultra Low Power e con limitate risorse di calcolo. Sfruttando il medesimo hardware si sono definite 3 tipologie di nodi:

- Il root node è il nodo che avvia il setup della rete e gestisce la creazione del grafo tramite l'invio del primo DIO, è il responsabile dell'acquisizione dei dati necessari per l'elaborazione della localizzazione e fornisce le informazioni circa il posizionamento dell'oggetto.
- L'anchor node è il dispositivo fisso che mantiene memoria dell'attenuazione ambientale tipica dello scenario applicativo e viene usato come riferimento dai nodi mobili durante le fasi di

localizzazione.

• Il Target node è collocato sui vari oggetti o persone che si vogliono tracciare e lavora tipicamente in modalità di sleep per salvaguardare le batterie. Il suo risveglio avviene solo quando interrogato circa la propria posizione o periodicamente nel caso si voglia tener traccia degli spostamenti dello stesso.

Accanto a queste tre tipologie è stato realizzato un nodo denominato Installation Target utilizzato soltanto in fase di installazione del sistema ed in particolare per fissare le caratteristiche in termini di propagazione dell'infrastruttura dove si è deciso di usare il sistema.

Una volta installata l'infrastruttura WiSeNet un numero tendenzialmente molto grande di target può entrare nello scenario ed essere localizzato all'interno dell'edificio. Nel dettaglio quando viene inviata la richiesta di localizzazione verso un determinato indirizzo IPv6 univoco questa si propaga nella rete fino al target, esso risponde con un ACK al root notificando l'avvenuta ricezione del messaggio ed avvia la procedura per la sua individuazione all'interno dell'edificio. Questa consiste nell'invio di una serie di pacchetti che verranno ricevuti dai soli anchor in visibilità, questi elaboreranno le informazioni circa l'RSSI ed invieranno il pacchetto dati al root che si occupa di fornire le coordinate del dispositivo all'interno dell'edificio preso in considerazione. Affinché la procedura vada a buon fine è necessario che si ricevano i pacchetti provenienti da almeno tre anchor node, altrimenti il meccanismo viene reiterato fino alla raccolta delle informazioni necessarie. In Figura 1 è riportata una mappa che rappresenta un'installazione in pianta stabile all'interno del Dipartimento di Ingegneria dell'Informazione dell'Università Politecnica delle Marche.

Nello specifico sono stati installati 9 anchor node capaci di coprire un'area di poco più di 1000 m^2. Sono stati eseguiti centinaia di test dai quali è risultato un errore massimo rispetto alla posizione realmente assunta dal target dell'ordine dei 2 metri ed un errore medio tipicamente inferiore al metro.

Il border router (molto spesso coincide con il root come in questo caso) consente di rendere i dati disponibili nel Cloud e permette le interrogazioni da remoto anche attraverso l'implementazione di una GUI molto semplice ed intuitiva da utilizzare.

Una ulteriore potenzialità del sistema è quella di permettere la connessione agli anchor o agli stessi target di una molteplicità di sensori utilizzabili sia per il monitoraggio ambientale, che per quello di parametri fisiologici se il target è una persona, che di parametri circa lo stato di un prodotto. Un esempio di quest'ultimo scenario sono quelle applicazioni di logistica e trasporto che coinvolgono materiali come possono essere gli alimenti notoriamente sensibili alle variazio-

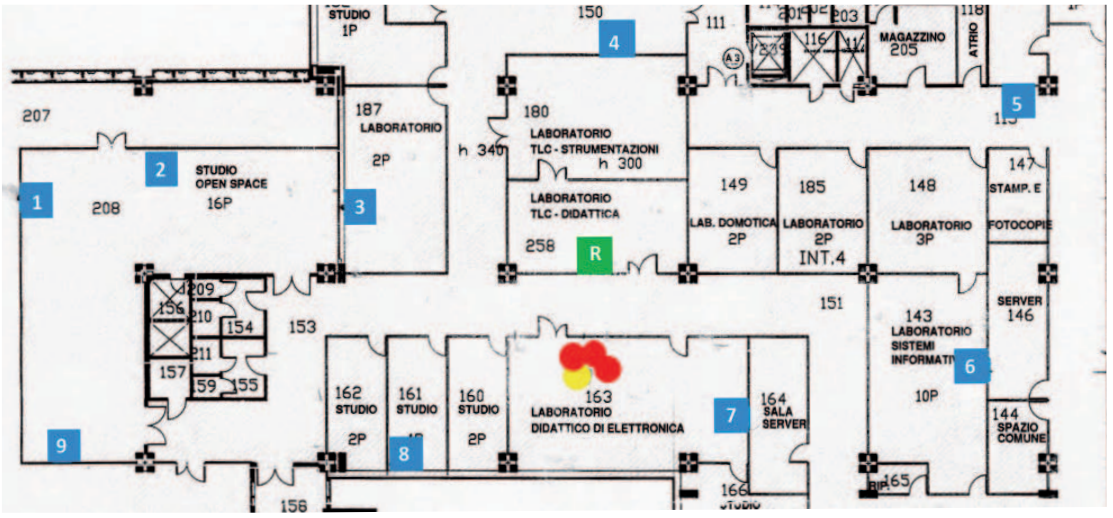
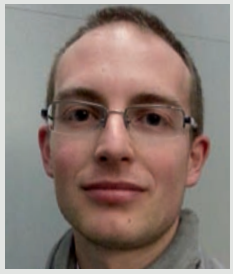


Fig.1 In blu gli anchor node installati, in verde la posizione del nodo root, in giallo la posizione reale di un target generico, in rosso la posizione stimata del target per 5 diverse richieste di localizzazione.

ni termiche o di umidità e la cui movimentazione deve seguire delle procedure regolamentate.

3. Conclusioni

La flessibilità, il ridotto consumo energetico, le dimensioni e la capacità elaborativa di WiSeNet consentono di adattarlo ai molteplici ambiti del mondo dell'IoT lasciando spazio ad ampi margini di sviluppo e customizzazione. Attualmente si stanno sviluppando delle API da fornire agli utilizzatori in modo tale che chiunque decida di affacciarsi al mondo dell'IoT abbia la possibilità di farlo in maniera semplice e veloce. Questo permetterà di creare la propria rete di Smart Object con il minimo investimento in termini sia economici che di tempo.



Lorenzo Palma
l.palma@univpm.it

Nel 2012 ha conseguito la Laurea Magistrale in Ingegneria Elettronica con voto 110/110 con Lode.
Nel 2013 ha avuto un contratto di collaborazione con Telecom in quanto vincitore di Working Capital 2012. Dal 2013 ha iniziato il corso di Dottorato di Ricerca nell'ambito dell'Internet of Things.

@unipi: centralizzazione del sistema di posta di Ateneo

Simone Spinelli

Università degli Studi di Pisa

Abstract. La pubblica amministrazione sta affrontando un momento di analisi e riorganizzazione delle proprie risorse IT con lo scopo di ottimizzare servizi e costi. Le scelte sulla gestione di servizi strategici come quello di posta elettronica non sono affatto scontate e devono tener conto degli aspetti economici e tecnologici. L'universita' di Pisa ha recentemente migrato i molti sistemi di posta presenti nell'Ateneo su una piattaforma centralizzata che uniforma e migliora i livelli di servizio rispondendo alle esigenze presenti e del prossimo futuro e che sopratutto lascia all'Ateneo pieno controllo dei dati e delle politiche applicate. Si tratta di una soluzione scale-out basata su software opensource interamente progettata e gestita con risorse interne della quale saranno trattati l'architettura, i componenti e i costi.

1. Scenario e obiettivi

La diffusione delle tecnologie di virtualizzazione e del paradigma cloud computing, ha portato profondi mutamenti nel modo di concepire e di utilizzare servizi come la posta elettronica trasformandoli in commodity. Nella pubblica amministrazione, si assiste ad un processo di ristrutturazione dei servizi IT che ha come obbiettivo quello di ottimizzare l'utilizzo delle risorse e di aumentare i livelli di servizio talvolta anche esternalizzandone alcuni come la posta elettronica. Anche l'Università di Pisa, nel corso dell'ultimo anno, ha avviato un processo di razionalizzazione e di normalizzazione che ha coinvolto sia le infrastrutture (di rete, di calcolo e di storage), che i meccanismi di erogazione e gestione dei servizi.

In passato, la gestione dei domini di posta elettronica nell'Ateneo pisano è stata spesso delegata ai singoli dipartimenti. Questo ha portato nel tempo alla proliferazione di una moltitudine di sistemi diversi fra loro in termini di affidabilità, prestazioni e modalità di erogazione del servizio. Per superare questo modello è nato il progetto @unipi, volto a centralizzare il servizio di posta elettronica e a migliorarne e uniformarne le caratteristiche complessive.

Il servizio è rivolto a tutta la comunità universitaria: il personale prima e gli studenti poi. In fase di progettazione sono state considerate le seguenti caratteristiche:

- Scalabilità in termini di numero di utenti e di dimensione della casella;
- 10 Gbyte di spazio per casella;
- Storage con possibilità di tiering;
- Continuità di servizio;
- Gestione dello spam;
- Utilizzo di soli protocolli sicuri e di autenticazione;
- Possibilità di cogestione del servizio con i tecnici dipartimentali;
- Meccanismi di disaster recovery [1];
- Valore giuridico della trasmissione [2].

2. Infrastruttura di computing

I servizi in gestione al settore SerRA si appoggiano su una infrastruttura di macchine virtuali distribuita su due datacenter nel centro cittadino. I siti sono collegati attraverso due anelli in fibra ottica che vengono utilizzati uno per l'esposizione dei servizi e l'altro per il traffico di storage e backup. Alimentazione, collegamenti di rete e storage utilizzano meccanismi di ridondanza e di alta affidabilità in modo da eliminare possibili SPOF. Seguendo la stessa filosofia, anche l'implementazione dei servizi viene fatta utilizzando meccanismi di alta affidabilità.

Per servizi che ospitano dati non ricostruibili, come l'hosting web o i server MDA, sono stati realizzati cluster di macchine virtuali ospitate

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

su volumi DRBD [3] replicati in tempo reale sui due datacenter: in ogni momento è possibile far migrare le istanze virtuali da un datacenter all'altro, ottimizzando così l'utilizzo complessivo delle risorse hardware e le prestazioni.
Nel caso di servizi in cui non è necessario preservare i dati o lo stato del sistema, come un DNS cache o una replica LDAP, sono stati utilizzati i meccanismi interni ai protocolli per la replica dei dati e bilanciatori LVS per l'alta affidabilità. Tutto il software utilizzato è opensource: i server fisici e virtuali hanno sistema operativo Linux Debian 6.0 o superiore, la tecnologia di virtualizzazione utilizzata è Xen [4], la replica in tempo reale dei dati viene fatta con DRBD, i cluster sono gestiti con Corosync/Pacemaker [5]e Linux LVS [6] viene utilizzato per i load balancer.

3. Il sistema

Nella progettazione del sistema si è cercato di disaccoppiare le varie componenti funzionali: posta in arrivo e in uscita, mailboxes, webmail, mappe e routing. Questa scelta agevola le operazioni di manutenzione e troubleshooting e permette di utilizzare i meccanismi di alta affidabilità più adatti al singolo servizio. Le componenti individuate sono:

- MTA posta in ingresso;
- MTA posta in uscita;
- MDA;
- Mappe/Routing;
- Webmail.

Al momento la piattaforma @unipi gestisce direttamente le circa 6000 caselle di posta elettronica del personale docente e tecnico amministrativo e il solo traffico di altre 70.000 degli studenti. In totale vengono impiegate 18 macchine virtuali escludendo quelle dedicate al servizio di Identity Management di Ateneo. Uno schema sintetico del sistema è rappresentato in figura 1.

3.1 MTA: posta in ingresso e in uscita

La posta in ingresso viene gestita da quattro server ad egual peso DNS: questo garantisce continuità di servizio e bilanciamento del carico. Il server SMTP utilizzato è Postfix [7].
Le connessioni in ingresso vengono gestite con Postscreen [8] che effettua i controlli di pregreeting (timing e rispetto dei protocolli) e sulle RBL (pesate). Successivamente si passa al blocco SMTP Access di Postfix che effettua i controlli pre-queue (validità di dominio e indirizzo destinatari) e poi a milter-greylist che applica le politiche di greylisting: in caso di assenza di un

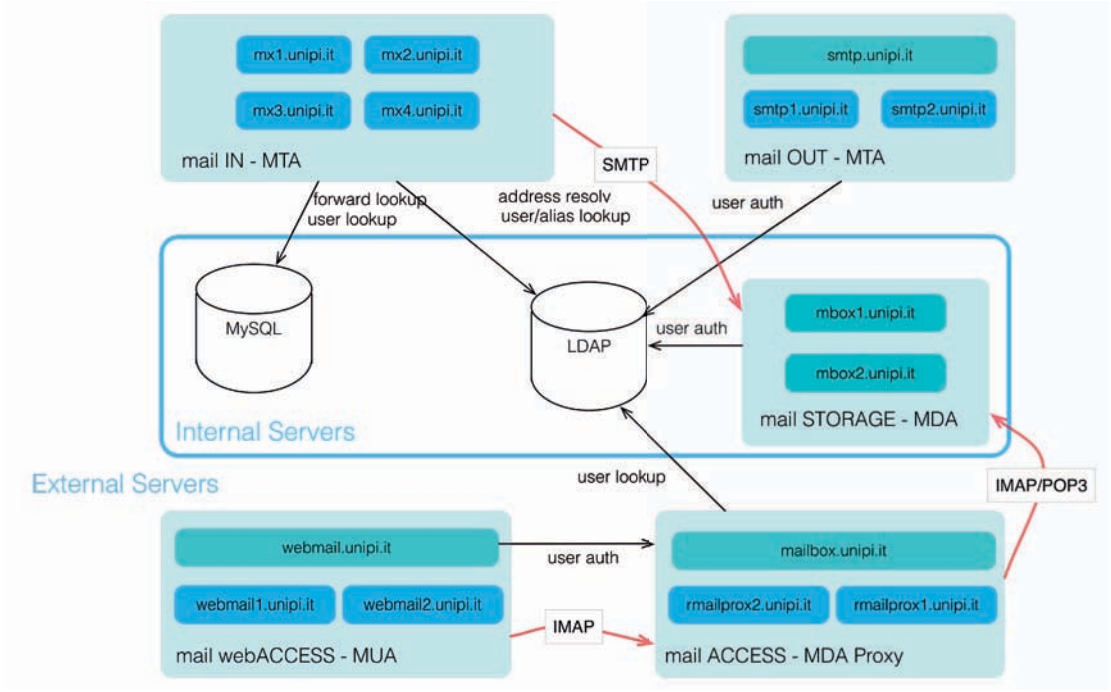


Fig.1 Schema sintetico del sistema

record SPF che indichi la politica da applicare, il server mittente viene messo in una whitelist temporanea, se invece un record SPF è presente, ne viene onorato il contenuto e la connessione viene accettata o rifiutata secondo la corrispondenza fra hostname del server e record SPF. Tutti i client segnalati in RBL che però non superano la soglia di blocco, vengono posti comunque in greylist.

Queste politiche sulle connessioni in ingresso abbattono fortemente il livello di spam e soprattutto il numero di messaggi che vengono analizzati: a fronte di circa un milione di connessioni giornaliere, solo 75.000 messaggi vengono effettivamente analizzati e di questi circa 5.000 vengono marcati o bloccati come spam.
L'analisi dei messaggi per l'applicazione delle politiche anti-spam e antivirus viene effettuata rispettivamente da Spamassassin e Clamav gestiti attraverso AmaVIS. La configurazione di Spamassin è impostata con soglie piuttosto alte: i messaggi vengono segnalati come spam se raggiungono un punteggio di almeno 6 e vengono bloccati con punteggio maggiore di 9. Anche per il learning bayesiano vengono utilizzate soglie alte: vengono considerati spam i messaggi con punteggio maggiore di 12 e ham quelli con punteggio minore di 2,3. È importante sottolineare nuovamente che l'utilizzo di soglie così conservative è possibile grazie all'implementazione di politiche molto rigide in fase di connessione.
Meccanismi antispam e antivirus similari vengono applicati anche sulla posta in uscita: questa scelta aiuta a mitigare il backscattering e ad individuare eventuali account compromessi. Il servizio di posta in uscita è realizzato con due server, esposti all'utenza tramite un bilanciatore e utilizzabili solo in modalità sicura e autenticata. L'utilizzo di un bilanciatore, in questo caso, permette di inserire o rimuovere nodi dal cluster senza disservizio percepibile: sia in caso di operazioni di manutenzione, sia nel caso un server venga compromesso o segnalato in RBL.

3.2 Backend: mappe, routing e identity management

Tutte le informazioni di routing sono mantenute su server specifici: le mappe postfix domain, access e gli alias con destinatari multipli, sono mantenute su un cluster MySQL composto da nodo master e due repliche utilizzate dai server MX: in questo modo si ottiene bilanciamento di carico e alta affidabilità. Un altro cluster MySQL viene utilizzato per i token di Spamassassin e viene popolato e acceduto da tutte le MTA (sia in ingresso che in uscita).

Oltre a fornire il servizio di autenticazione e autorizzazione per l'accesso alla rete e ai servizi, la directory di Ateneo viene utilizzata anche per l'erogazione del servizio di posta. A questo scopo è stata creata una objectClass privata per l'inserimento di attributi specifici per il servizio di posta fra cui indirizzo, alias personali, quota e server MDA di appartenenza.

I server LDAP vengono, quindi, interrogati dai server di posta in ingresso sia per la risoluzione degli alias personali che per la risoluzione degli indirizzi nella forma <username@server_mailbox> (contenuto nell'attributo unipiMailHost) necessaria per la corretta consegna in casella.

Questa soluzione ha permesso di utilizzare differenti server mailbox e quindi di realizzare la scalabilità orizzontale del sistema tramite user sharding.

3.3 MDA: storage e accesso alle caselle

Una volta noto il server MDA di destinazione, il messaggio viene spedito via SMTP al server mailbox di destinazione dove un demone postfix lo consegna a Dovecot [9], l'MDA che si occupa del salvataggio del messaggio in casella.

I server MDA in uso attualmente sono due e sono realizzati con macchine virtuali Xen su volumi DRBD replicati sui due datacenter (con RAID6 locale). Ognuno dei server ha 5TB di spazio disco per le mailbox.

Il frontend per l'accesso alle caselle tramite IMAP/PoP (solo via SSL/TLS) è garantito da un cluster di proxy Dovecot che mascherano all'utente il vero server mailbox di destinazione: il proxy reindirizza la connessione verso il nodo corretto interrogando LDAP (attributo unipiMailHost) e l'utente viene autenticato direttamente sul server di appartenenza. Per questo servizio è stato usato il bilanciamento DNS su due VIP gestiti dal cluster: in caso di fault di un nodo, il vip assegnato migra su uno

dei nodi rimasti. Il servizio di webmail è realizzato utilizzando due server roundcube bilanciati tramite LVS

4. Gestione

L'integrazione con la piattaforma di identity management è essenziale per il provisioning delle risorse: l'attivazione di un indirizzo o un alias personale diventa una operazione che viene fatta sulla piattaforma stessa. Per la gestione di alias a destinazione multipla e per le mappe ospitate su SQL viene utilizzata una semplice interfaccia RubyOnRails. Per il tracciamento dei messaggi e per il trobleshooting è stato realizzato un sysylog server centralizzato che mantiene gli ultimi tre mesi di log, a questo se ne affianca un altro per il mantenimento dello storico (1 anno). L'utilizzo di software aperti permette di utilizzare strumenti standard e facilmente automatizzabili quali ldap-tools, imapsync, rsync, SQL. Le migrazioni dai sistemi dipartimentali a quello centralizzato sono state fatte con questi strumenti che verrano utilizzati in fase di espansione del sistema e che sono usati per realizzare i meccanismi di backup. In questo modo un piccolo set di strumenti standard permette di gestire l'intera piattaforma in tutti i suoi aspetti, dal mantenimento all'espansione. Il sistema in questione è comunque piuttosto complesso e articolato, basti pensare al numero totale di istanze virtuali: gli strumenti di automazione (Rex [10]) e configuration management (Git [11]) hanno svolto e svolgonoo un ruolo essenziale per la gestione, il deploy e lo sviluppo.

5. Analisi dei costi

Sebbene un'analisi dei costi puntuale sia al di fuori degli scopi di questo documento, è possibile fare alcune considerazioni per avere delle indicazioni relative all'investimento iniziale e ai costi nel tempo. Dato che il software in uso non ha alcun costo di licenza, verranno considerati solo i costi relativi all'infrastruttura fisica (server e network) e al consumo energetico. A questi occorre sommare il costo del personale che si può considerare quello di due unità impiegate al 50% (1FTE).

Mentre sono facilmente identificabili i costi relativi allo storage (i dischi sono dedicati), è più difficile calcolare l'incidenza del sistema di posta in termini di risorse di computing e network. Si può però ipotizzare di utilizzare come fattore moltiplicativo il rapporto fra le macchine virtuali dedicate alla posta elettronica e le macchine virtuali attive sull'infrastruttura fisica. Per il network si considera il numero di macchine virtuali attive sull'intera infrastruttura (175), per il computing viene considerato solo il numero di macchine virtuali attive su sistemi fisici sui quali vengono ospitate anche le istanze che compongono il sistema di posta (85).
Fatte queste considerazioni, i risultati sono riassunti dalla tabella seguente:

	Spesa	Incidenza	Spesa posta elettronica
Network	40K €	10%	4K €
Computing	24K €	20%	4.8K €
Infrastruttura fisica	15K €	10%	1.5K €
Totale (escluso storage)	79K €		
Storage			18K €
Totale			28.3K €

Quelli identificati fino ad ora vanno intesi come costi di startup. Occorre ora considerare il tempo di vita del sistema stesso che si può fissare a 5 anni: questo, infatti, è il periodo per il quale l'hardware è coperto da assistenza.

Considerando quindi le spese relative al magazzino hardware (circa 5k euro una tantum) e quelle di assorbimento energetico (circa 6KW per l'intera infrastruttura) si ottiene un costo annuo di circa 1,2 euro/casella. Questo calcolo è fatto considerando le attuali 5.000 caselle attive, ma se il sistema si espandesse a 10.000 caselle, il costo si abbatterebbe a 60cents/casella.

6. Conclusioni e sviluppi futuri

Come per l'investimento fatto a suo tempo sulle infrastrutture di rete, anche sul fronte dei servizi l'Ateneo pisano ha affrontato la sfida con risorse interne: questo ha permesso di mantenere il possesso completo dei dati e del know-how necessario, a fronte di un costo di start-up senza dubbio consistente, soprattutto in termini di im-

pegno professionale, ma che permette nel tempo di crescere secondo le necessità e di mantenere il controllo delle politiche applicate.

Il futuro dell'infrastruttura di posta di Ateneo si sviluppa lungo due direttrici: l'attivazione di nuovi servizi e strumenti che permettano una gestione multi-tenant della piattaforma e lo sviluppo di una soluzione di object-storage basata su CEPH capace di supportare le strutture di ricerca, il personal cloud e un servizio di posta per gli studenti con caratteristiche similari a quello offerto al personale di Ateneo. Lo storage utilizzato per la posta elettronica andrà quindi a rappresentare una parte relativamente piccola di quello utilizzato per la ricerca, la gestione documentale e il personal cloud e questo abbasserà ulteriormente i costi di gestione.

In conclusione, riteniamo che i servizi strategici debbano essere sviluppati e gestiti dalle divisioni IT delle Università. Il valore strategico della posta elettronica non è rappresentato solo dai dati personali contenuti nei messaggi, dalle relazioni che la corrispondenza esprime ma anche, e soprattutto, dalla possibilità di gestire le politiche del servizio, adattandole alle proprie esigenze e mantenendone pieno controllo.

Riferimenti bibliografici

[1] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/continuita-operativa

[2] http://archivio.digitpa.gov.it/cad/valore-giuridico-della-trasmissione

[3] http://drbd.linbit.com

[4] http://www.xenproject.org

[5] http://clusterlabs.org/doc

[6] http://www.linuxvirtualserver.org

[7] http://www.postfix.org

[8] http://www.postfix.org/POSTSCREEN_README.html

[9] http://www.dovecot.org

[10] http://www.rexify.org

[11] http://git-scm.com

Simone Spinelli
simone.spinelli@unipi.it

Dottore in Ingegneria delle Telecomunicazioni, lavora come System Administrator presso l'Università di Pisa – settore SerRA dal 2002. Si è occupato, tra l'altro, dei servizi di monitoring e di telefonia di Ateneo. Al momento segue lo sviluppo delle infrastrutture di storage e cloud computing.

IPv4-in-IPv6: una nuova strategia per la transizione a IPv6

Massimo Vellucci[2], Massimo Bernaschi[1], Luca Vollero[2]

[1] *CNR-IAC, Istituto per la Applicazioni del Calcolo*
[2] *Università Campus Bio-Medico di Roma*

Abstract. IPv4 è il protocollo di comunicazione adottato dalla maggioranza dei dispositivi collegati a Internet. Tuttavia, essendo un protocollo definito nelle prime fasi dello sviluppo di Internet, il suo utilizzo pone problemi legati all'esaurimento degli indirizzi IPv4 disponibili e ad altre sue limitazioni costitutive. IPv6 è la nuova versione del protocollo Internet, definita con l'obiettivo di superare i limiti di IPv4.
La sfida principale nella diffusione di IPv6 è data dalla disponibilità di meccanismi efficaci per l'integrazione dei servizi attivi in reti IPv4 su reti IPv6, minimizzando i costi ed i rischi connessi alla migrazione.
Il presente lavoro propone un nuovo meccanismo basato sul tunneling dinamico di pacchetti IPv4 in IPv6 e denominato, per questo, IPv4-in-IPv6. L'approccio proposto è rivolto agli operatori di rete che vogliono semplificare la configurazione e la gestione del loro backbone IPv6, mantenendo il pieno supporto di IPv4 sulle reti di accesso.

1. Introduzione

IPv4, (1) è il protocollo di comunicazione adottato dalla maggioranza dei dispositivi collegati a Internet. Tuttavia, essendo un protocollo definito nelle prime fasi dello sviluppo di Internet, il suo utilizzo pone dei problemi legati all'esaurimento degli indirizzi IPv4 disponibili e ad altre sue limitazioni costitutive in ambito di mobilità e sicurezza. IPv6, (2), detto anche IP next generation (IPng), è la nuova versione del protocollo Internet, definita con l'obiettivo di superare i limiti di IPv4. Il problema principale nella migrazione a IPv6 è legato al gran numero di applicazioni e servizi Internet basati su IPv4, che non sopravvivrebbero a una banale sostituzione di protocollo. La sfida principale nella diffusione di IPv6, dunque, si traduce nella disponibilità di meccanismi efficaci per l'integrazione dei servizi attualmente attivi in reti IPv4 su reti IPv6 (3), minimizzando i costi ed i rischi connessi alla migrazione (4).

Con lo scopo di facilitare una graduale integrazione tra IPv4 e IPv6, il Working Group IPng Transition (ngtrans) della IETF (Internet Engineering Task Force) ha analizzato le questioni legate a tale transizione (5) e ha proposto diversi meccanismi, che costituiscono un "transition toolbox" (6), volti a facilitare l'interoperabilità tra i due protocolli e la migrazione a IPv6. Il presente lavoro propone un nuovo meccanismo basato sul tunneling dinamico di pacchetti IPv4 in IPv6 e denominato, per questo, IPv4-in-IPv6. Tale meccanismo si aggiunge a quelli disponibili nel suddetto "transition toolbox". L'approccio proposto è rivolto agli operatori di rete che vogliono semplificare la configurazione e la gestione del loro backbone IPv6, mantenendo il pieno supporto di IPv4 sulle reti di accesso e per i data center che necessitano di un ritardo per l'introduzione del nuovo protocollo

2. La soluzione IPv4-in-IPv6

2.1 Stato dell'arte nelle soluzioni di tunneling IPv4 over IPv6

La maggior parte delle soluzioni di tunneling prevede la gestione di flussi IPv6 incapsulati in tunnel IPv4 (6) (7) (8) (9) (10) (11) (12), e fa riferimento a scenari in cui la transizione è all'inizio e si ha la necessità di collegare isole IPv6 per mezzo di un'infrastruttura IPv4. Più recentemente, sono state proposte diverse soluzioni che si basano sul tunneling opposto, con lo scopo di gestire scenari in cui IPv6 è il protocollo dominante nell'infrastruttura di rete. Queste soluzioni si basano prevalentemente sulle specifiche di tunneling su IPv6 definite in (13). L'aspetto principale che differenzia questi meccanismi di tunneling è la configurazione del tunnel IPv4-over-IPv6 e la gestione del processo

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

di incapsulamento:

- 4in6 (13) è l'approccio più semplice e si basa sulla configurazione manuale di tunnel statici combinati con una conversione di indirizzo stateless. 4in6 può essere combinato con il Tunnel Setup Protocol (TSP) (14) al fine di facilitare la configurazione dei tunnel in un'infrastruttura complessa.
- La tecnica 4rd (15) prevede l'impiego di tunnel IPv4-over-IPv6 costruiti per associazione stateless di indirizzi IPv4 o coppie indirizzi IPv4/porta sugli indirizzi IPv6 utilizzati come end-point del tunnel. Questo permette ai pacchetti IPv4 di attraversare un dominio 4rd attraverso dei tunnel automatici IPv4-over-IPv6.
- Il Dual-Stack Lite (DS Lite) (16) è una soluzione che unisce l'incapsulamento del traffico IPv4 in tunnel IPv6 con la tecnica Network Address Translation (NAT) e consente a un fornitore di servizi di condividere i medesimi indirizzi IPv4 tra più clienti. DS Lite è un modello dedicato agli ISP che vogliono realizzare un'infrastruttura completamente basata su IPv6 e, nello stesso tempo, vogliono fornire ai loro utenti anche connettività IPv4.
- Infine, 4over6 (17) è un altro meccanismo pensato per consentire a un backbone IPv6 di gestire flussi IPv4. Sotto 4over6 ogni nuvola IPv4 è dotata di un router dual stack che gestisce l'incapsulamento di flussi IPv4, mentre l'estensione Multiprotocol Extension del protocollo Border Gateway Protocol (BGP-MP) (18) (19) è utilizzata per inoltrare i dati necessari alla creazione dei tunnel 4over6 tra i router.

Le soluzioni sopra descritte presentano delle limitazioni che possono influenzare sensibilmente la loro applicabilità in scenari reali. 4in6 è statico e manca di flessibilità nelle infrastrutture di grandi dimensioni in cui l'informazione sugli end-point disponibili è non controllabile in modo centralizzato e fortemente variabile. DS Lite si basa su NAT e presenta il problema del mascheramento dell'indirizzo IP degli utenti finali. In 4rd e 4over6 l'incapsulamento è delegato a nodi specifici, facilitando la configurazione automatica e la gestione dei tunnel, ma introducendo dei punti critici nella rete. Inoltre, 4rd e 4over6 non sono progettati per fornire tunnel tra differenti AS e questo rende impraticabile il collegamento di nodi IPv4 appartenenti a differenti AS se non collegati tramite IPv6.

2.2 La proposta IPv4-in-IPv6

L'approccio IPv4-in-IPv6 proposto nel presente lavoro è basato su quattro aspetti principali: la gestione degli indirizzi IP, l'incapsulamento dei flussi IPv4, la configurazione e gestione dei tunnel e la generazione dei messaggi di errore.

Gestione degli indirizzi IP

IPv4-in-IPv6 richiede l'impiego dedicato di una classe IPv6 di indirizzi pubblici. Nel seguito assumeremo che tale classe sia la 2005::/16. L'utilizzo di tale classe consente la configurazione di tunnel con end-point situati anche su due AS distinti. La generazione di un indirizzo IPv6 avviene prendendo il prefisso prescelto e aggiungendo nella parte meno significativa l'indirizzo IPv4.

Incapsulamento / Decapsulamento

IPv4-in-IPv6 assume che ogni rete di accesso IPv4 disponga di un dispositivo IPv4-in-IPv6, gestito dal provider di servizi Internet (ISP) e che colleghi tale rete al backbone IPv6 (1). Questo dispositivo è responsabile del tunneling IPv4. Quando un pacchetto IPv4 viene inviato attraverso questo dispositivo, quest'ultimo si occupa di incapsulare automaticamente il pacchetto in un pacchetto IPv6. L'incapsulamento è basato su (13), con indirizzi di origine e di destinazione costruiti tramite la regola spiegata al punto precedente. Dopo l'incapsulamento, il pacchetto viene quindi trasmesso attraverso il backbone IPv6. Quando un pacchetto IPv6 raggiunge un dispositivo IPv4-in-IPv6 nella rete di destinazione, questo viene controllato per determinare se contiene un flusso IPv4. Se gli indirizzi sorgente/destinazione del pacchetto appartengono alla classe in uso per flussi incapsulati e se il pacchetto contiene effettivamente un pacchetto IPv4, l'apparato decapsula il pacchetto. Dopo la fase di decapsulamento, il pacchetto viene inoltrato attraverso la rete locale IPv4.

Configurazione e gestione dei tunnel

La configurazione e la gestione dei tunnel è automatica e dinamica, cioè l'instaurazione di un tunnel non richiede protocolli di segnalazione tra i due end-point e non sono richiesti protocolli di controllo per la gestione dei tunnel in caso di riconfigurazione della rete. Ogni tunnel IPv4-in-

IPv6 è basato interamente sui normali meccanismi di routing. La raggiungibilità di una sottorete IPv4 all'interno del backbone IPv6 è consentito dall'annuncio di una determinata rotta (tramite i comuni protocolli di routing) dal relativo router PE che gestisce tale rete IPv4. E' compito del router PE connesso ad una sottorete IPv4 annunciare la raggiungibilità della sottorete IPv6 gestita tramite IPv4-in-IPv6. Per esempio, per permettere il tunneling automatico dei pacchetti IPv4 verso la sottorete IPv4 a.b.c.0/24, il router PE annuncerà se stesso come destinatario dei pacchetti della sottorete 2005::a.b.c.0/120.

Gestione errori mediante ICMP e gestione MTU

Gli errori rilevati fuori dai tunnel IPv6 sono segnalati direttamente con il protocollo ICMPv4 (20). Di contro, gli errori rilevati durante l'invio di un pacchetto IPv6 contenente un pacchetto IPv4 vengono segnalati tramite il protocollo ICMPv6 (21). In questo caso è necessaria la traduzione in ICMPv4 se l'errore si riferisce alla comunicazione del tunnel IPv4. In questo caso, la traduzione viene effettuata dall'end-point sorgente. Inoltre, quando un pacchetto IPv4 entra in un tunnel e la dimensione del pacchetto originale supera la MTU gestita dal tunnel, l'end-point sorgente scarta il pacchetto e restituisce un messaggio ICMPv4 di host non raggiungibile causato da un pacchetto troppo grande. In questo caso il nodo IPv4 sorgente, informato che i suoi pacchetti superano la MTU del tunnel, può reagire riducendo la dimensione dei pacchetti inviati.

2.3 Implementazione

La soluzione proposta è stata implementata sotto forma di un modulo del kernel Linux, e appare come un'interfaccia di rete virtuale. Tale modulo può essere installato all'interno di ogni nodo di rete che vuole supportare direttamente entrambi i protocolli. Nella nostra implementazione, le tabelle di routing dei nodi di incapsulamento rispettano le seguenti regole:

- Nei nodi di incapsulamento IPv4-in-IPv6 la tabella di routing IPv4 è configurata in modo che la rotta predefinita del traffico IPv4 inoltri il traffico verso il dispositivo di rete virtuale. Non appena un pacchetto IPv4 indirizzato a un host remoto raggiunge questo nodo, viene inviato sull'interfaccia virtuale tramite la rotta predefinita. Il modulo kernel IPv4-in-IPv6 entra in azione costruendo il corrispondente pacchetto IPv4-in-IPv6 e lo accoda sullo stack di rete dell'IPv6. Alla fine il pacchetto IPv4-in-IPv6 è gestito dalla tabella di routing IPv6 e trasmesso al prossimo hop all'interno del backbone IPv6.
- Nei nodi di decapsulamento IPv4-in-IPv6 la tabella di routing IPv6 è configurata in modo tale che per ogni rete IPv6 associata ad una rete IPv4 sia presente un'interfaccia di rete virtuale che si occupa di incapsulare e decapsulare i pacchetti di rete. Non appena un pacchetto IPv6 indirizzato a una di tali reti raggiunge il nodo IPv4-in-IPv6, esso lo inoltra al dispositivo di rete virtuale. Il modulo kernel IPv4-in-IPv6 entra nuovamente in azione estraendo il pacchetto IPv4 dal pacchetto IPv4-in-IPv6 e accodandolo sullo stack di rete IPv4. Alla fine il pacchetto IPv4 viene inoltrato al destinatario tramite la tabella di routing IPv4.

3. Prestazioni del modulo sviluppato

Il modulo software è stato sottoposto a sperimentazione per verificarne la correttezza funzionale e le prestazioni in un ambiente di rete reale. In particolare, è stato implementato un test-bed costituito da oltre 50 tra apparati di rete e host di comunicazione. Nel test-bed ogni apparato di rete e ogni host è una macchina virtuale configurata e gestita in un server VMware ESXi. In particolare il test-bed, rappresentato in Fig. 1, è costituito da 4 AS, ognuno implementato in un diverso server VMware. Le connessioni interne agli AS sono virtuali e gestite mediante VMware, mentre le connessioni tra AS sono effettive. La sperimentazione ha riguardato due aspetti fondamentali: la stabilità del modulo software e le prestazioni ottenibili su tunnel IPv4-in-IPv6.

3.1 Stabilità del modulo software

Il primo test effettuato ha riguardato la stabilità del modulo software. Il test ha previsto la configurazione di 3 comunicazioni TCP tra AS differenti (AS2_DC1_HOST1 -> AS1_DC2_HOST2, AS3_DC3_HOST1 -> AS1_DC1_HOST4, AS4_DC1_HOST3 -> AS1_DC1_HOST1) tenute attive per 2 giorni di fila. A valle dell'esperimento è stata effettuata un'analisi dei log di sistema e una verifica dello stato di funzionamento delle macchine coinvolte e del modulo software. Dall'analisi dei sistemi e dei log si è verificato il corretto funzionamento dei sistemi e una comunicazione senza

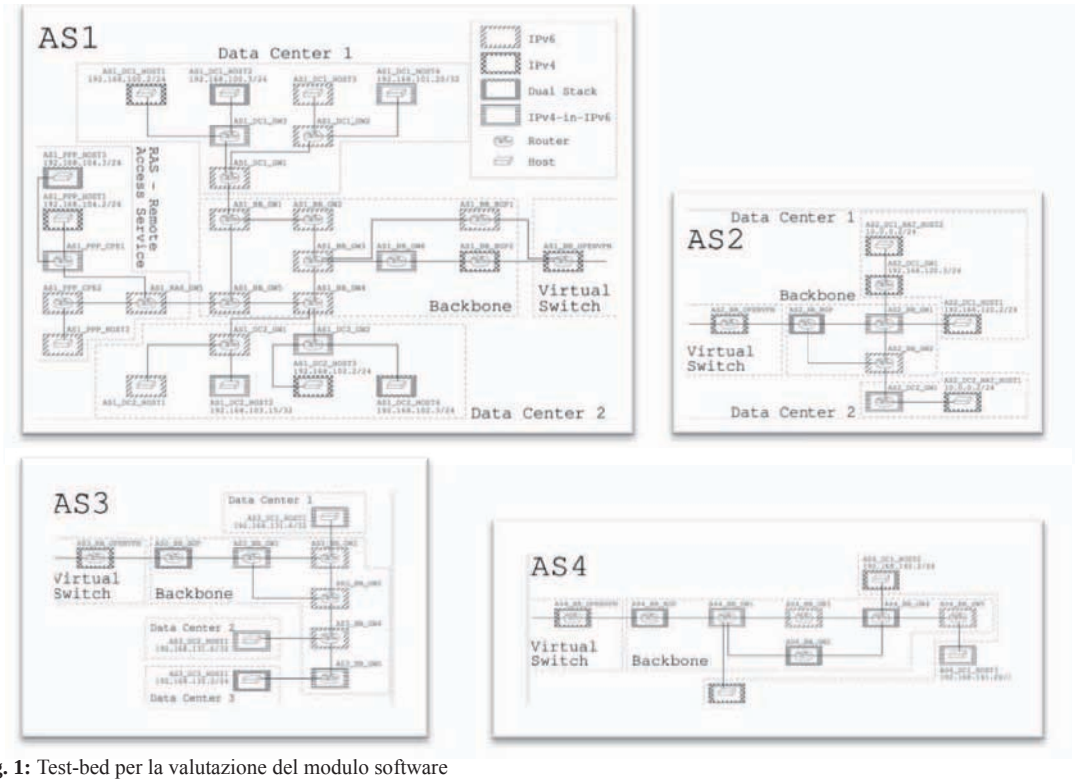


Fig. 1: Test-bed per la valutazione del modulo software

errori al massimo throughput di comunicazione.

3.2 Prestazioni

I successivi test hanno riguardato la stabilità e l'analisi delle prestazioni del modulo implementato. Un primo test è stato realizzato tra due host reali collegati mediante uno switch a 100Mbps. I due host sono stati configurati per comunicare in due condizioni diverse: (i) mediante IPv4 direttamente e (ii) mendiante IPv4 ma passando per il modulo IPv4-in-IPv6. La comunicazione tra gli host ha previsto la creazione di un canale TCP mandato in saturazione mediante un trasferimento FTP. L'analisi del traffico ha evidenziato un calo di prestazioni, imputabile essenzialmente all'overhead di IPv4-in-IPv6, sotto il valore di 1.5% del throughput.

Un secondo test ha riguardato l'instaurazione di diverse comunicazioni tra host dell'AS1 di Fig. 1 al fine di verificare il corretto funzionamento e le prestazioni del modulo software per tutte le possibili combinazioni di incapsulamento. In questo contesto, alcuni host sono stati configurati come server e sono stati dotati di server HTTP (lightHTTP nello specifico), mentre gli host client sono stati configurati per interrogarli e generare un trasferimento dati (mediante wget). I trasferimenti dati sono stati monitorati con tcpdump e registrati. I risultati medi su tre trasferimenti sono riportati in Tab. 1, dove sono anche indicati gli host sorgente

N.	Client	HTTP Server	Throughput (Mbps)-Packet Rate (pkts)	Connessione
1	AS1_DC2_HOST2	AS1_DC1_HOST4	1.74-9928/1.80-10254	IPv4/IPv6
2	AS1_DC2_HOST2	AS1_DC1_HOST2	1.86-10533/1.75-10015	IPv4/IPv6
3	AS1_DC2_HOST2	AS1_DC1_HOST1	1.88-10669	IPv4
4	AS1_DC2_HOST3	AS1_DC1_HOST4	1.73-9864	IPv4
5	AS1_DC2_HOST3	AS1_DC1_HOST2	1.80-10259	IPv4
6	AS1_DC2_HOST3	AS1_DC1_HOST1	1.74-9913	IPv4
7	AS1_DC2_HOST4	AS1_DC1_HOST4	1.71-9801/1.79-10244	IPv4/IPv6
8	AS1_DC2_HOST4	AS1_DC1_HOST2	1.75-9978/1.74-9909	IPv4/IPv6
9	AS1_DC2_HOST4	AS1_DC1_HOST1	1.72-9797	IPv4

Tab. 1 Risultati dei test di valutazione delle prestazioni

e destinazione dei flussi dati. Per tutte le configurazioni, il modulo ha operato in modo stabile, con prestazioni adeguate ai link configurati tra i vari host (10 Mbps).

4. Conclusioni

Nel presente lavoro abbiamo presentato una nuova strategia per la transizione a IPv6, basata sulla costruzione dinamica di tunnel IPv4-in-IPv6. Tale strategia, oltre a essere presentata, è stata implementata e valutata sperimentalmente. Come nota a margine, il modulo software è stato portato con successo in un apparato di rete reale: il FRITZ!Box per WLAN 7390.

Riferimenti bibliografici

[1] K. Nichols, S. Blake, F. Baker, D. Black. "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" RFC 2474 (Proposed Standard). 1998.

[2] Hinden, S. Deering, R. "Internet Protocol, Version 6 (IPv6) Specification" RFC 2460 (Draft Standard). 1998.

[3] M. Mackay, C. Edwards, M. Dunmore, T. Chown, G. Carvalho. "A scenario-based review of IPv6 transition tools" Internet Computing, IEEE, vol. 7, pp. 27 – 35. 2003.

[4] Carpenter, B. "IPng White Paper on Transition and Other Considerations" RFC 1671 (Informational). 1994.

[5] Haskin, R. Callon, D. "Routing Aspects of IPv6 Transition" RFC 2185 (Informational). 1997.

[6] Gilligan, E. Nordmark, R. "Basic Transition Mechanisms for IPv6 Hosts and Routers" RFC 4213 (Proposed Standard). 2005.

[7] Moore, B. Carpenter, K. "Connection of IPv6 Domains via IPv4 Clouds" RFC 3056 (Proposed Standard). 2001.

[8] A. Durand, P. Fasano, I. Guardini, D. Lento. "IPv6 Tunnel Broker" RFC 3053 (Informational). 2001.

[9] Jung, B. Carpenter, C. "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels" RFC 2529 (Proposed Standard). 1999.

[10] F. Templin, T. Gleeson, D. Thaler. "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)" RFC 5214 (Informational). 2008.

[11] Templin, F. "Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces" RFC 5579 (Informational). 2010.

[12] Troan, W. Townsley, O. "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification" RFC 5969 (Proposed Standard). 2010.

[13] Deering, A. Conta, S. "Generic Packet Tunneling in IPv6 Specification" RFC 2473 (Proposed Standard). 1998.

[14] Parent, M. Blanchet, F. "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)" RFC 5572 (Experimental). 2010.

[15] R. Depres, S. Matsushima, T. Murakami, O.Troan. "IPv4 Residual Deployment across IPv6-Service networks (4rd) ISP-NAT's made optional". 2011.

[16] A. Durand, R. Droms, J. Woodyatt, Y. Lee. "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion" RFC 6333 (Proposed Standard). 2011.

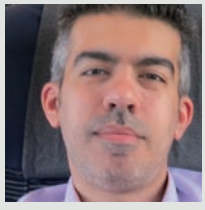
[17] J. Wu, Y. Cui, X. Li, M. Xu, C. Metz. "4over6 Transit Solution Using IP Encapsulation and MP-BGP Extensions" RFC 5747 (Experimental). 2010.

[18] Y. Rekhter, T. Li, S. Hares. "A Border Gateway Protocol 4 (BGP-4)" RFC 4271 (Draft Standard). 2006.

[19] T. Bates, R. Chandra, D. Katz, Y. Rekhter. "Multiprotocol Extensions for BGP-4" RFC 4760 (Draft Standard). 2007.

[20] Postel, J. "Internet Control Message Protocol" RFC 792 (Standard). 1981.

[21] A. Conta, S. Deering, M. Gupta. "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification" RFC 4443 (Draft Standard). 2006



Massimo Vellucci
m.vellucci@unicampus.it

Massimo Vellucci si è laureato al corso di Informatica (Vecchio Ordinamento) presso l'Università La Sapienza di Roma (2006). Attualmente ricopre il ruolo di responsabile delle infrastrutture IT dell'Università Campus Bio-Medico di Roma. L'attività di ricerca si sviluppata principalmente nell'ambito del networking e reti wireless.

Workshop GARR_14 - *Selected papers*

ISBN 978-88-905077-5-5